Информационная безопасность (кибербезопасность) для школьников и их родителей: как защитить ребёнка в цифровом мире

Жамьянов А.М.

заместитель начальника департамента связи и информатизации мэрии города Новосибирска

Мэрия города Новосибирска
Департамент связи и информатизации

Почему это важно — цифры и вызовы в 2025 году

Каждый **2-й (3-й в 2024)** школьник столкнулся с киберугрозой *(Минпросвещения РФ, аналитика Роскомнадзора, 2025)*

81% (72% в 2024) детей не рассказывают родителям о проблемах в сети *(ВЦИОМ)*

+40% за год рост мошенничества через мессенджеры и игры *(МВД РФ, отчёт «Киберпреступность против несовершеннолетних», январь 2025)*

Мэрия города Новосибирска
Департамент связи и информатизации

Топ-5 угроз для школьников в 2025 году

«Приучите ребёнка не выдавать личную информацию в чатах»

Мэрия города Новосибирска
Департамент связи и информатизации

Указ Президента РФ от 7 мая 2024 г. № 309 «О национальных целях развития РФ»

Среди 11 показателей достижения национальной цели «Цифровая трансформация госуправления, экономики и социальной сферы» к 2030 году одним из показателей является - создание системы эффективного противодействия киберпреступлениям и снижения ущерба от их совершения.

1

- Создание антифрод-платформы взаимодействия онлайн госорганов, банков, МФО, операторов связи и цифровых платформ.

2

- Развитие технологий выявления мошеннических и фишинговых сайтов, кибербезопасность на основе ИИ.

3

- Развитие технологий обеспечения безопасности ключевой сетевой инфра- структуры и борьбы с DDoS.

4

- Внешняя оценка защищенности ключевых ГИСов.

5

- Борьба с «серыми» сим-картами и введение оборотных штрафов за утечки персональных данных.

Мэрия города Новосибирска
Департамент связи и информатизации

Концепция информационной безопасности детей. Что важно знать?

Утверждена Правительством РФ 28 апреля 2023 г. № 1105-р — основа всех региональных программ, включая Новосибирск.

🎯 Стратегическая цель:

Развитие безопасного информационного пространства и защита детей от деструктивного воздействия.

Ключевые принципы:

- Ведущая роль государства и приоритетная ответственность родителей.
- Защита традиционных духовно-нравственных ценностей.
- Формирование у детей критического мышления и цифровой грамотности.
- Безопасность использования интернета в образовательных организациях.

Мэрия города Новосибирска
Департамент связи и информатизации

Бесплатные курсы на Stepik — учимся всей семьёй!

Для школьников 6–9 классов:

- **Курс «Безопасность в интернете»** — 3 модуля, видео + тесты, 2 часа
- **Курс «Информационная безопасность для школьников»** — Wi-Fi, пароли, мошенники

Для старшеклассников и родителей:

- **Курс «Математика в кибербезопасности»** — как математика защищает от хакеров
- **Курс : «Основы цифровой безопасности»** — 34 модуля, финтех, фишинг

✓ **Курсы бесплатные, с сертификатами**
✓ **Можно проходить вместе с ребёнком — семейный формат**

Мэрия города Новосибирска
Департамент связи и информатизации

Что могут сделать родители — 5 простых шагов

Настройте родительский контроль — Kaspersky Safe Kids

Обсудите правила цифровой жизни — «Никогда не отправляй данные/фото незнакомцам»

Пройдите курс на Stepik вместе с ребёнком — и обсудите, что узнали

Создайте «цифровой ужин» — 1 раз в неделю без гаджетов — только разговоры

Знайте, куда обратиться — школьный психолог, горячая линия 8-800-2000-122

УРОК ЦИФРЫ

ОБЪЯСНЯЕМ.РФ

stepik

С мобильных телефонов короткий номер 124
ТЕЛЕФОН ДОВЕРИЯ
8 800 2000 122
ДЛЯ ДЕТЕЙ, ПОДРОСТКОВ И ИХ РОДИТЕЛЕЙ

Мэрия города Новосибирска
Департамент связи и информатизации

Реальные кейсы и потенциал для Новосибирска

01

Курс Stepik

«Безопасность в интернете» уже прошли **>50 000** школьников по РФ — **89%** улучшили знания по защите данных.

02

IT-Кубы по РФ

средняя посещаемость мастер-классов для родителей — **85–95%**.

По опыту Москвы внедрение курсов по цифровой грамотности снизило обращения по кибербуллингу на **22%**. *Источник: mos.ru*

✓ **Наша цель в Новосибирске:**
достичь таких же или лучших показателей к 2025 году.

Мэрия города Новосибирска
Департамент связи и информатизации

Что делает Новосибирск в 2025-2026?

Интеграция модулей ИБ в школьную программу — кружки, внеурочные занятия.

Разработка концепции цикла обзорной образовательной программы для школьников от Департамента Связи и информатизации мэрии города Новосибирска.

Обучение сотрудников и ИТ-специалистов по стандартам ФСТЭК. Обучение. Осознанность. Осведомленность.

Мэрия города Новосибирска
Департамент связи и информатизации

Отечественный мессенджер MAX

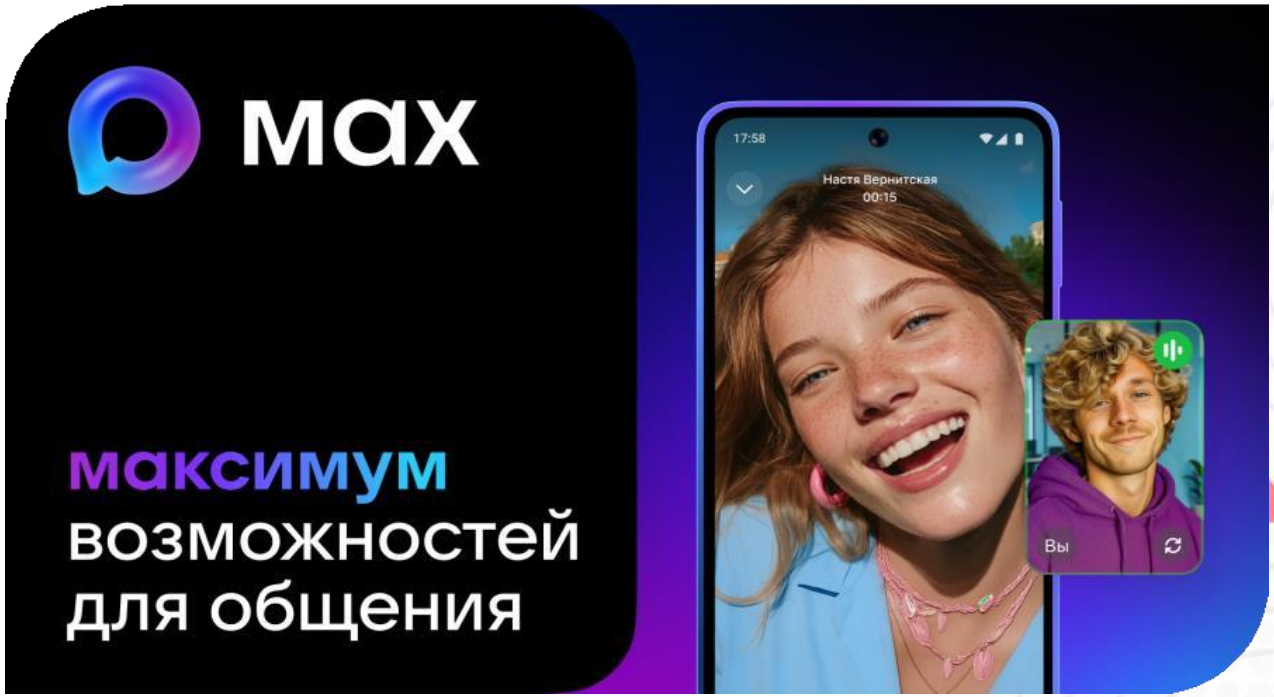
Российский мессенджер MAX

Чаты УК с жителями

Сервис цифрового МФЦ в MAX

Перевод школьного общения в MAX

Каналы и сообщества
Создан канал Губернатора НСО и Новосибирь



max

Советы от экспертов — что говорят психологи и IT-специалисты?

- **«Не запрещайте — объясняйте. Ребёнок должен понимать "почему", а не бояться "наказания"»** — детский психолог, Новосибирск.

- **«Лучшая защита — это осведомлённость. Учите ребёнка задавать вопросы»** — эксперт по ИБ, Stepik.

- **«Родительский контроль — это не слежка, это обучение»** — методист Департамента образования.

Мэрия города Новосибирска
Департамент связи и информатизации

Основные угрозы информационной безопасности

Фишинг

Поддельные электронные письма, мошеннические сайты.

Мошенничество

Кража личных данных, финансовое мошенничество.

Кража личных данных

Фишинг, взлом паролей, несанкционированный доступ к данным.

- **Фишинг** — это вид интернет-мошенничества, при котором злоумышленники пытаются получить доступ к личным данным пользователей, таким как пароли, номера кредитных карт и т. д. Они отправляют поддельные письма от имени известных компаний или государственных органов, чтобы убедить пользователей предоставить свои личные данные.
  Чтобы защититься от фишинга, необходимо быть внимательным и осторожным при работе в интернете. Не открывайте подозрительные письма и не переходите по ссылкам, если вы не уверены в их подлинности. Используйте антивирусное программное обеспечение и обновляйте его регулярно.
- **Мошенничество** — ещё одна серьёзная угроза информационной безопасности. Злоумышленники могут использовать различные методы мошенничества, такие как кража личных данных, финансовое мошенничество и другие. Они могут украсть ваши личные данные, например, номер кредитной карты, адрес электронной почты и пароль, и использовать их для совершения незаконных действий.
- **Кража личных данных** — это ещё одна распространённая угроза информационной безопасности. Она может привести к финансовым потерям, нарушению конфиденциальности и другим негативным последствиям. Злоумышленники могут украсть ваши личные данные различными способами, такими как фишинг, взлом паролей и другие.

Мэрия города Новосибирска
Департамент связи и информатизации

Кибербезопасность — это просто!

Важно знать:

- Как создать надёжный пароль
- Как защитить мобильное устройство
- Как не стать жертвой фишинга
- Как распознать звонок мошенника
- Что рассказать детям о кибербезопасности
- Что рассказать людям старше 60 лет

Мэрия города Новосибирска
Департамент связи и информатизации

Признаки надёжного пароля

- **Длинный и сложный** - 12 символов: используйте буквы в разном регистре, цифры и специальные символы: `~!@#$%^&*+-/.,\{}[]();:|?<>=`

- **Избегайте последовательностей** - не используйте простые комбинации вроде «qwerty» или «12345». Создавайте «случайные комбинации» букв, цифр и символов.

- **Без личных данных** - не включайте фамилию, дату рождения, кличку питомца или другую информацию, доступную в соцсетях.

- **Используйте фразы** - пароли на основе фраз сложнее угадать, но легче запомнить.
- Пример: - ГотовлюБорЩ_на5+баллов!@ - Прохождение$Цивилизации-1час - Поеду1_вРио-де-Жанейро-вБелыхШт@н@х.

- **Уникальность** - для каждого важного сервиса (банк, соцсети, Госуслуги) придумайте свой пароль. Если в сервисе нет критичных данных, можно использовать простой пароль, даже повторяющийся.

Надёжный пароль = защита ваших данных!

Мэрия города Новосибирска
Департамент связи и информатизации

Как защитить свой мобильный телефон

- 🔒 **Создание сложного пароля:** Используйте длинный пароль или PIN-код, состоящий из букв, цифр и символов.
- 📱 **Двухфакторная аутентификация:** Включите двухфакторную аутентификацию для защиты учетных записей.
- 🛡️ **Антивирусные программы:** Установите антивирусное ПО для защиты от вредоносного программного обеспечения.
- 🔄 **Регулярные обновления:** Обновляйте операционную систему и приложения до последних версий.
- 🚫 **Ограничение доступа к приложениям:** Настройте ограничения на доступ к важным приложениям через биометрию или дополнительные пароли.
- 🌐 **Безопасный Wi-Fi:** Подключайтесь только к защищенным сетям Wi-Fi и избегайте общедоступных точек доступа.
- 👀 **Контроль за приложениями:** Проверяйте разрешения приложений перед их установкой и регулярно очищайте список установленных программ.
- 🗑️ **Удаленное управление устройством:** Активируйте функцию удаленного управления для блокировки устройства или удаления данных в случае утери.

Мэрия города Новосибирска
Департамент связи и информатизации

Как не стать жертвой фишинга

Внимательно проверяйте адрес отправителя

🔍 Адреса сайтов могут незначительно отличаться от настоящих. Будьте внимательны!

Не переходите по подозрительным ссылкам в сообщениях

⚠ Проверяйте ссылки перед тем, как переходить по ним. Избегайте рекламных баннеров на сомнительных сайтах.

Проверяйте информацию из рассылок

📨 Всегда перепроверяйте информацию на официальных источниках. Не доверяйте письмам без проверки.

Меняйте пароли в самом сервисе

🔒 Никогда не переходите по ссылкам для смены паролей. Делайте это только через официальный сайт или приложение.

Скачивайте программы из официальных магазинов приложений

📱 Обращайте внимание на рейтинги и отзывы. Для программ банков, попавших под санкции, используйте официальные сайты.

Сообщайте о подозрительных письмах на рабочей почте

Перед открытием вложений свяжитесь с отправителем. Сообщайте о подозрительных письмах в службу безопасности.

Повышайте киберграмотность

🎓 Пройдите курсы по кибербезопасности и регулярно тестируйте свои навыки.

Мэрия города Новосибирска
Департамент связи и информатизации

Как создать учётную запись ребёнка на Госуслугах

- **Внимание!** Перед привязкой необходимо создать и подтвердить учетную запись ребенка от 10 до 17 лет, это может сделать сам ребенок после получения паспорта.
- Учётная запись ребёнка на Госуслугах — это личный кабинет для детей до 17 лет включительно. Она создаётся одним из родителей с подтверждённой учётной записью и автоматически привязывается к его личному кабинету.
- Создать учётную запись онлайн на Госуслугах можно, если у ребёнка есть СНИЛС и свидетельство о рождении, выданное в России или российских консульствах. Если у ребёнка иностранный документ о рождении, обратитесь в центр обслуживания для создания карточки ребёнка в вашем личном кабинете. После этого можно самостоятельно создать учётную запись из своего личного кабинета.