Развитие критического мышления как основа курса кибербезопасности для школьников: какое содержание работает

Алексей Васильевич Конобеев, к.пед.н.,
ст.н.с. ФГБНУ ИСМО, доцент МПГУ,
академический директор Умскул

Тревожная статистика

- С 2022 по 2024 год количество зарегистрированных IT-преступлений выросло почти в 1,5 раза — с 522,1 тысячи до 765,4 тысячи случаев.
- финансовый ущерб от киберпреступлений за три года составил почти 390 миллиардов рублей, рост: с 91 миллиарда рублей в 2022 году до 200 миллиардов в 2024-м.
- взрывной рост вовлечения несовершеннолетних как в совершение киберпреступлений (увеличение в 74 раза за период 2020-2023 годов), так и их виктимизация, с более чем двукратным ростом пострадавших детей в 2025 году.
- Ключевой новый тренд: для создания дипфейков в целях буллинга стали активнее применять технологии искусственного интеллекта (только за период ноябрь 2025 — январь 2026 года выявили порядка 1,5 тысячи таких эпизодов

Несовершенные жертвы киберпреступоений

- за январь-июль 2025 года почти 5 тысяч детей и подростков стали жертвами IT-преступлений, что на 25% больше, чем за аналогичный период 2024 года. За девять месяцев 2025 года количество несовершеннолетних, пострадавших от киберпреступлений, возросло на 120% по сравнению с аналогичным периодом предыдущего года.
- в 2024 году почти 17 тысяч несовершеннолетних были признаны потерпевшими.
- По данным опроса сервиса RWB (сентябрь 2025 года), с мошенничеством или опасными ситуациями в сети сталкивались 18% детей в возрасте 5–17 лет. При этом риск растет с возрастом: среди детей 5–7 лет таких случаев было 5%, а среди подростков 14–17 лет — уже 26%. В 2025 году киберполиция отмечала: фокус мошенников сместился в сторону молодежи и цифровых схем, ориентированных на подростков
- общий ущерб от таких преступлений с начала 2025 года может превышать 850 миллионов рублей. Средний размер ущерба вырос более чем вдвое — с 80 тысяч рублей в начале года до 190 тысяч рублей к октябрю.

Опасность не только для детей

- россияне в возрасте от 25 до 44 лет чаще всего становятся жертвами мошеннических действий киберпреступников. Банк России составил типичный портрет жертвы киберпреступников в 2024 году — это работающая женщина (36,1% опрошенных) в возрасте 25-44 лет, проживающая в городе и имеющая средний уровень дохода и образования.
- на втором месте находятся люди в возрасте от 45 до 64 лет (27,5%).
- около 20% от общего числа жертв мошенников в России составляют россияне старше 60 лет, при этом 17% киберпреступлений совершаются непосредственно в отношении пенсионеров.
- идет снижение возраста пострадавших: в 2024 году среди жертв было около 2 тысяч человек в возрасте от 18 до 30 лет, а в 2025 году - 3 тысячи.

Как научить защищаться

Почему, несмотря на обучение средствам компьютерной безопасности, количество жертв растет?

Почему все новые люди попадают в ловушки мошенников?

Корни проблемы

- обычно основное внимание в обучении - на аппаратных средствах защиты (антивирус, двухфакторная аутентификация).
- пока знакомим со способами работы мошенников, те уже придумывают новые.
- у детей и подростков недостаточно развито системное мышление, психологи отмечают “клиповость”, мозаичность мышления, неспособность соотнести то, чему учат в школе, в тем, что происходит в жизни.

Основа безопасности - критическое мышление

Важно уметь вовремя понять:

- что информации не стоит доверять;
- что информацию надо проверить;
- что вами манипулируют;
- что разговор или переписку надо закончить, при необходимости очень твердо.

Типичные уловки мошенников

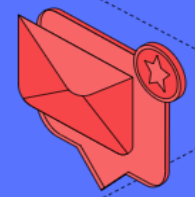
- “дай поиграть с твоего аккаунта, а я тебе заплачу”;
- “деньги можно легко заработать”
- “никто тебя не понимает так, как я. Сейчас скажу что тебе надо делать”
- “ты ничего плохого не делаешь”;
- “ты несовершеннолетний, тебе ничего не будет”;
- “если ты этого не сделаешь, то… (угрозы)”

Помимо нехватки критического мышления, есть недостаточное правосознание.

Актуальность

Современные подростки ежедневно сталкиваются с разнообразными онлайн-угрозами — от фейковых новостей и кликбейта, ведущих на вредоносные сайты или тексты, вовлекающие в правонарушения, до фишинга, дипфейков и кибермошенничества, а также могут быть вовлечены в террористическую деятельность силами злоумышленников.

Развитие искусственного интеллекта, социальных сетей и цифровых коммуникаций делает приёмы мошенников всё изощрённее — а значит, их сложнее распознать

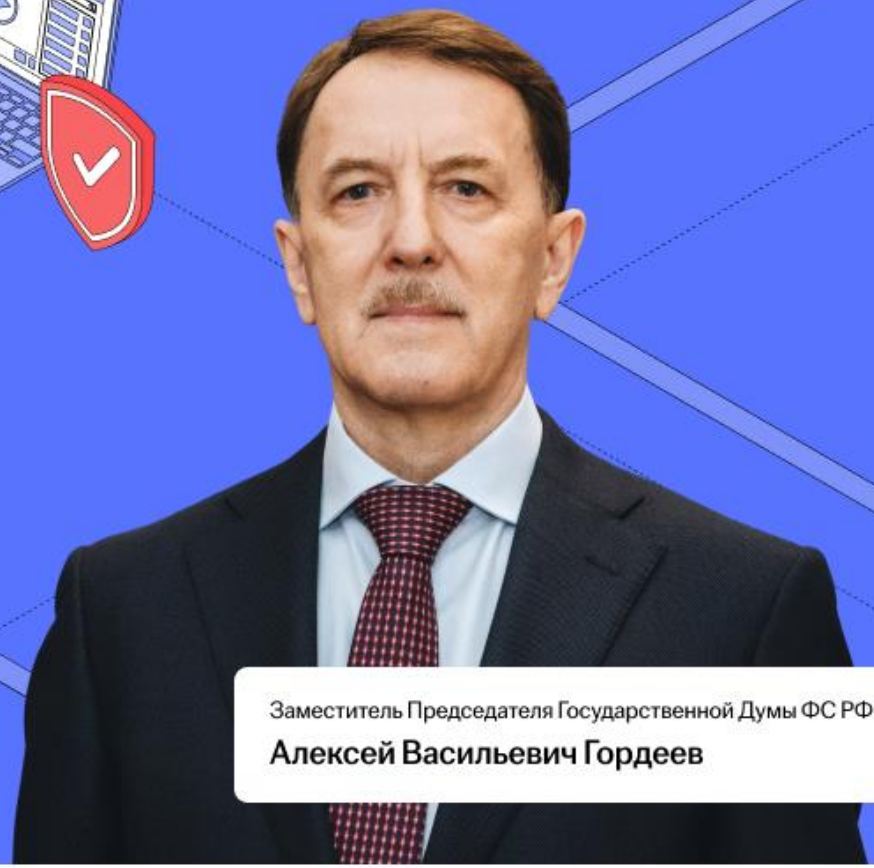


Умскул

Бесплатный онлайн-курс

«Кибербезопасность: учимся защищаться»

Проект реализован по инициативе заместителя Председателя Государственной Думы ФС РФ Алексея Васильевича Гордеева



Заместитель Председателя Государственной Думы ФС РФ
Алексей Васильевич Гордеев

Создано при содействии:

Федеральной службы безопасности России

Министерства внутренних дел по Республике Башкортостан

Министерства внутренних дел по Воронежской области

Министерства образования Воронежской области

ВИРО

Института образования Воронежской области

Общероссийский народный фронт

Народного фронта России

Курс “Кибербезопасность: учимся защищаться”

Объем курса - 14 академических часов

Разделы курса:

- Раздел 1 Критическое мышление и борьба с речевыми манипуляциями - 4 ак.ч.
- Раздел 2 Фейки, фишинг и дипфейки - 2 ак.ч.
- Раздел 3 Кибермошенничество и правовая грамотность - 3 ак.ч.
- Раздел 4 Цифровая гигиена и защита данных - 2 ак.ч.
- Раздел 5 Противодействие вербовке в деструктивные сообщества - 2 ак.ч.
- Раздел 6 Научи родителей - 1 ак.ч.

Компоненты курса: уроки на платформе, конспекты уроков, рабочая тетрадь, методические рекомендации, программа курса

От развития мышления - к действиям

Логика построения курса обеспечивает поступательное развитие компетенций в рамках деятельностного системного подхода: базовые навыки критического мышления → распознавание конкретных угроз → практические навыки защиты → трансляция знаний другим.

Возможные формы провдения

- В классе
- В гибридном формате (часть учеников подключаются онлайн)
- Самостоятельная работа

ВАЖНО: у каждого ученика прогресс выполнения отображается индивидуально, при просмотре видео в классе, фронтально, важно просить школьников посмотреть видео и выполнить интерактивные задания самостоятельно (*есть в некоторых уроках)

Структура урока

1. **Введение** — актуализация темы, постановка проблемы
2. **Основная часть** — изучение теоретического материала через видеоурок, обсуждение ключевых вопросов, анализ примеров
3. **Практическое задание** — отработка навыков на конкретных кейсах, ролевых играх, практических упражнениях
4. **Рефлексия** — обсуждение усвоенного материала, формулирование выводов
5. **Домашнее задание** — закрепление материала, подготовка к следующему уроку

Типовая структура урока

1. Организационный этап (2–3 минуты)

- приветствие обучающихся
- проверка готовности к уроку (наличие рабочих тетрадей, доступа к устройствам при необходимости)
- краткая проверка домашнего задания или актуализация материала предыдущего урока

2. Мотивационный этап (3–5 минут)

- постановка проблемной ситуации, связанной с темой урока
- обсуждение реального случая из новостей или практики
- формулирование цели урока совместно с обучающимися
- создание мотивации через демонстрацию практической значимости темы

Пример (урок 8 «Актуальные схемы кибермошенничества»):
"На прошлой неделе в нашем городе было зафиксировано 15 случаев мошенничества с участием подростков. Как вы думаете, почему школьники становятся жертвами мошенников? Сегодня мы научимся распознавать схемы обмана и защищаться от них."

Типовая структура урока

3. Основной этап (25–30 минут)

Просмотр видеоурока (18-25 минут)

- включение видеоурока на проекторе или интерактивной доске
- обучающиеся могут делать краткие заметки в рабочих тетрадях
- педагог следит за вниманием группы

Обсуждение ключевых вопросов (5–7 минут)

- фронтальное обсуждение содержания видеоурока
- уточняющие вопросы от обучающихся
- объяснение сложных моментов педагогом
- установление связи между теоретическим материалом и практикой

Практическая работа (10–15 минут)

Типовая структура урока

Формы практической работы зависят от темы урока:

Анализ кейсов (уроки 4, 7, 8, 9, 12, 13):

- педагог представляет реальную ситуацию (текстовое описание, аудиозапись звонка мошенника, скриншот сообщения)
- обучающиеся в группах по 3–4 человека анализируют ситуацию
- каждая группа выявляет признаки угрозы, определяет возможные последствия, предлагает варианты защиты
- группы презентуют свои выводы, класс обсуждает

Ролевые игры (уроки 8, 9, 12, 13):

- педагог распределяет роли (мошенник/вербовщик и потенциальная жертва)
- пары проигрывают диалоги
- остальные обучающиеся наблюдают и анализируют
- обсуждение: что было сделано правильно, что можно улучшить
- проигрывание ситуации с учётом рекомендаций

Типовая структура урока

Практические задания с использованием устройств (уроки 2, 3, 5, 10, 11):

- обучающиеся работают на своих устройствах (планшетах) или школьных компьютерах
- выполняют конкретные действия: проверяют новость на достоверность, настраивают приватность в соцсетях, создают надёжный пароль
- педагог оказывает индивидуальную помощь
- обсуждение результатов, обмен опытом

Групповая работа над проектом (урок 14):

- деление класса на группы по 3–4 человека
- каждая группа создаёт памятку для родителей на выбранную тему
- работа с шаблонами, подбор информации, оформление
- подготовка к презентации

Типовая структура урока

4. Контрольно-оценочный этап (5–7 минут)

- выполнение контрольного задания (индивидуально или в парах)
- самопроверка по эталону (при наличии)
- взаимопроверка в парах
- обсуждение типичных ошибок

Примеры контрольных заданий:

- урок 2: проверить достоверность 2 новостей, указав использованные инструменты
- урок 4: определить манипулятивные приёмы в 3 рекламных текстах
- урок 10: создать надёжный пароль по изученным правилам

Типовая структура урока

4. Контрольно-оценочный этап (5–7 минут)

5. Рефлексивный этап (3–5 минут)

- обсуждение итогов урока через вопросы:
  - Что нового вы узнали сегодня?
  - Что было самым сложным/интересным?
  - Как вы сможете применить эти знания в жизни?
  - Какие вопросы остались?
- краткое резюме педагога с акцентом на ключевых выводах
- объяснение домашнего задания с критериями выполнения
- ответы на вопросы обучающихся

Подробные рекомендации

Этап 1. Ввод в тему

1. Вопрос к классу:
   «Всегда ли можно доверять информации, полученной от других людей? В каких случаях информация может требовать проверки?»
2. Короткое обсуждение: почему необходимо быть готовым проверять информацию.
3. Обозначить задачу на просмотр:
   «Во время видео попробуйте:
   – записать причины и виды когнитивных искажений;
   – записать виды логических ошибок».

Этап 2. Просмотр видео (длительность видео - 18 минут)

- Сразу дать установку: «Смотрим не “фоном”, а как исследователи: всё, что кажется важным, — фиксируем».
- По необходимости сделать 2 короткие паузы:
  - после блока про критическое мышление и стратегии мышления — уточнить, всё ли понятно с примерами;
  - после блока про логические ошибки — спросить, сталкивались ли с подобным.

Подробные рекомендации

Этап 3. Обсуждение содержания

1. Мини-опрос (устно или на доске): какие виды логических ошибок запомнили?
   – апелляция к авторитету;
   – ложная причинно-следственная связь;
   – скользкая дорожка;
   – атака на личность;
   – апелляция к невежеству;
   - эффект ореола;
   - социальный стереотип.
1. Проверяем себя по файлу с конспектом занятия
2. Краткое обсуждение логических ошибок: какие виды показались наиболее распространенными и опасными. Скажите ученикам, что мы еще вернемся к этой теме когда будем обсуждать речевые манипуляции.

Этап 4. Практика

Выполняем задания в рабочей тетради

Этап 5. Рефлексия и домашнее задание

- Записать примеры логических ошибок, с которыми встретитесь в жизни до следующего урока.

Важно: не вместо, а вместе

Информатика:

- основы информационной безопасности
- защита информации и цифровых устройств
- работа с сетевыми сервисами
- технологии искусственного интеллекта

Обществознание:

- правовые основы цифрового пространства
- права и обязанности граждан
- социальные отношения в цифровой среде
- гражданская ответственность

Важно: не вместо, а вместе

Право:

- Федеральный закон о защите персональных данных (152-ФЗ)
- Уголовный кодекс РФ (статьи о кибермошенничестве, экстремизме, терроризме)
- Закон о защите детей от информации, причиняющей вред здоровью

Психология:

- критическое мышление
- методы психологического воздействия и манипуляции
- принятие решений в условиях неопределённости
- противостояние давлению

Важно: не вместо, а вместе

Основы безопасности жизнедеятельности (ОБЗР):

- угрозы в цифровой среде
- алгоритмы безопасного поведения
- обращение в экстренные службы

Русский язык и литература:

- анализ текстов
- выявление манипулятивной риторики
- создание собственных текстов (памятки, инструкции)

Курс создан

Специалистами Умскул (концепция курса - А.В. Конобеев, к.пед.н., академический директор Умскул, старший научный сотрудник ФГНБУ “ИСМО”, доцент МПГУ)

при участии

- Специалистов ФСБ
- Специалистов МВД
- Психологов
- Специалистов по информационной безопасности
- Специалистов Народного фронта и Кибердружины

Как подключиться учителю

Две видеоинструкции:

- как подключиться с мобильного устройства https://drive.google.com/file/d/1K-q8eSTmOb3z5aaaVREmgrvwJgDk8WbC/view?usp=sharing
- как подключиться с компьютера https://drive.google.com/file/d/1DaCi7yomm_9swvNq-EEM7z0fjXQNad80/view?usp=sharing

Обе инструкции на лендинге курса https://landing.umschool.net/kiberbez_get_course

Как подключиться учителю

Доступ педагога к материалам курса Кибербезопасность:

1. проходим по ссылке https://landing.umschool.net/kiberbez
2. Пролистываем до конца страницы, нажимаем красную кнопку ПОЛУЧИТЬ КУРС.
3. Переходим по еще одной указанной на платформе ссылке в раздел ПОДГОТОВКА К ОГЭ/ЕГЭ, регистрируемся на платформе, следуя выпадающим указаниям.
   После регистрации открывается страница с перечнем классов (5, 6, 7...), выбираем 7 класс, далее выбираем ЛЮБЫЕ ТРИ ПРЕДМЕТА ВНУТРИ 7 класса, после этого вверху появляется поле ИСПОЛЬЗОВАТЬ ПРОМОКОД, сюда вставляем из памяти скопированный заранее промокод, переходим по нему.
4. Открываются материалы курса, которые надо СРАЗУ скачать, так как промокод ОДНОРАЗОВЫЙ, пройти по нему второй раз не получится.

Как контролировать работу ученика

- Заполненные рабочие тетради (или ведут записи в своих тетрадях)
- участвуют в обсуждениях на уроке
- при необходимости могут показать со своего устройства что уроки просмотрены, интерактивные задания выполнены

Какие материалы можно скачать

Можно: рабочие тетради, конспекты уроков

Нельзя: видео (авторские права)

Результаты пилотирования курса

- В феврале-апреле 2026 года на территории Воронежской области онлайн-курс прошли более **16 000** семиклассников, с которыми работали более **650** педагогов области.
- По результатам опроса 590 учеников, средняя оценка полезности составила **9,1/10**, а понятности материала — **9,3/10.** Практические умения освоили **94%** респондентов, а готовность применять знания на практике достигла **96%**. Уровень осознания юридической ответственности за киберправонарушения - **87%**. Индекс лояльности - **98,5%** готовы рекомендовать курс..
- По мнению 35 опрошенных педагогов, курс демонстрирует высокие показатели качества: средняя оценка полезности материалов составила **9,2/10,** актуальности примеров — **9,1/10**. Новизну контента педагоги оценили в среднем на **8,4/10**, что подтверждает ценность предлагаемых знаний для образовательного процесса. **98%** учителей подтвердили оптимальный уровень сложности курса для целевой аудитории (7 класс), а **89%** отметили сбалансированное соотношение теории и практики. Полноту охвата ключевых тем кибербезопасности подтвердили 98% респондентов («полностью» или «в целом достаточно»).

Результаты пилотирования курса

- Региональная олимпиада по кибербезопасности: более 1500 учеников 7 классов школ Воронежской области, апрель-май 2026 года.
- 2 тура - отборочный и очный финал (командные задания)
- Финальный тур: два практикоориентированных задания. Первое – «Реальные кейсы». Участникам необходимо было проанализировать жизненные ситуации, в которых подростки пострадали от действий киберпреступников. Получив карточку с описанием конкретного случая, команды разрабатывали план действий, который поможет не попадаться на уловки мошенников в будущем. Случаи отличались от тех, которые были использованы в курсе.
- Второе задание – «Аналитики кибербезопасности». Школьники попробовали себя в роли экспертов: им предстояло объяснить заданной аудитории (родителям, дедушкам и бабушкам, пятиклассникам) как распознать угрозы в Сети и предложить способы защиты.

Результаты пилотирования курса

Результаты апробации курса и олимпиады подтвердили эффективность методической концепции, отбора материалов, способов обучения и всего курса.

Курс остается бесплатным, и вы можете его использовать.

https://landing.umschool.net/kiberbez

Полезные материалы для учителя

https://max.ru/id1655451687_4_bot

- Методические материалы
- Развивающий курс для школьников
- Приемы для достижения метапредметных результатов
- и многое другое

Полезные ресурсы

Издание будет полезно для школьных учителей и преподавателей колледжей и вузов по любым предметам, желающих научиться применять нейросети для планирования уроков, создания учебных и контрольных материалов, в том числе текстовых, визуальных, аудиоматериалов, а также освоить принципы работы с любыми нейросетями. Основное внимание в издании уделено методическим особенностям применения нейросетей и решению конкретных задач в образовательном процессе. Для широкого профессионального сообщества.

https://prosv.ru/product/neiroseti-dlya-uchitelya-prosto-o-poleznom208768801/

АВГУСТ ПРО
образование, регион, развитие

сообщество для учителей VK

сообщество для учителей TG

Алексей Васильевич Конобеев
к.пед.н., ст.н.с. ФГБНУ ИСМО,
академический директор Умскул