

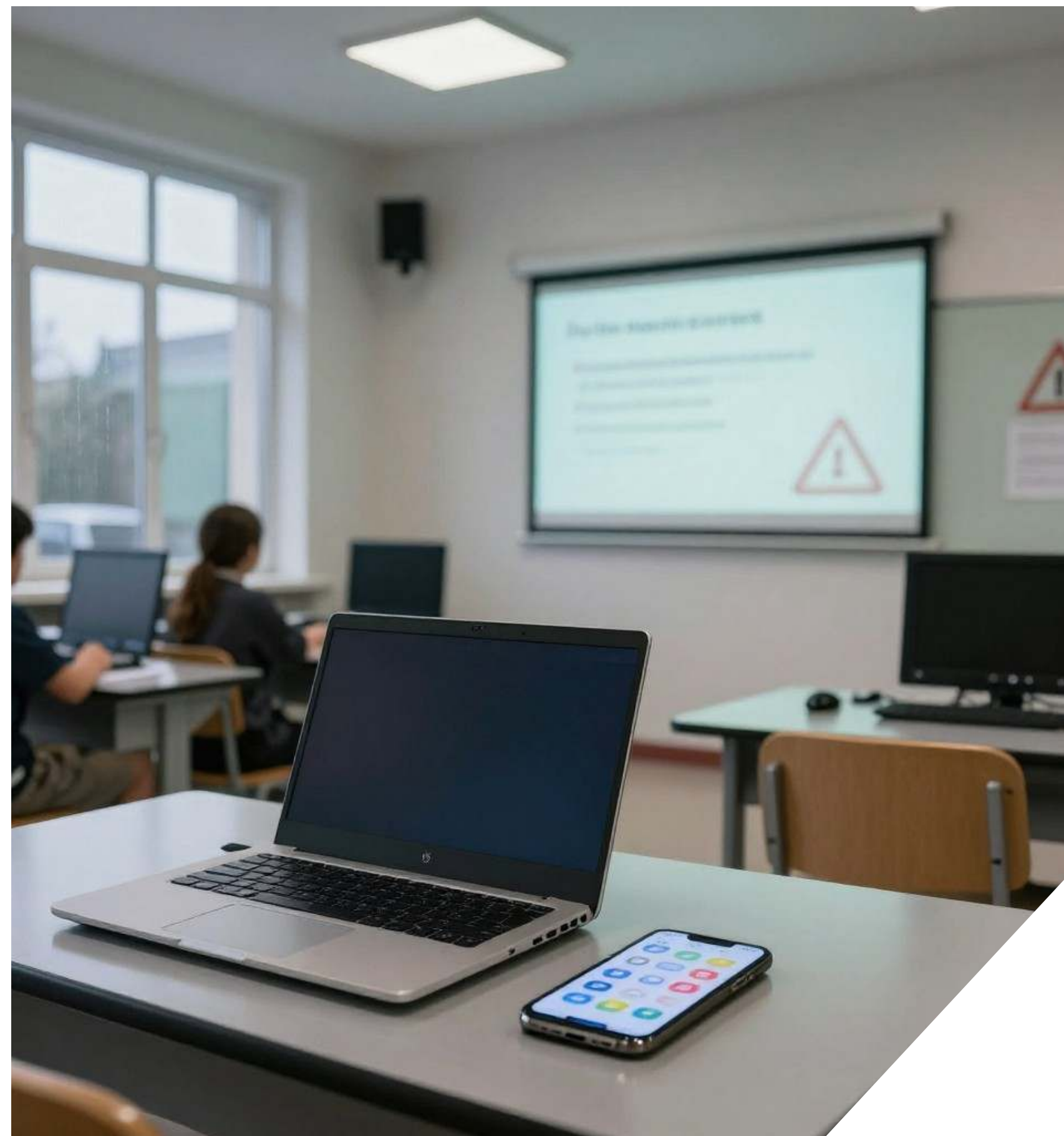
Интернет: как пользоваться безопасно и разумно

Интернет даёт пользу, но несёт
риски. Разберём личные данные,
незнакомцев и цифровой след.



-
- > Почему эта тема важна для семиклассников

В 7 классе ученики чаще общаются в мессенджерах, соцсетях, смотрят видео и играют онлайн. Опыта распознавания обмана ещё мало. Самые частые проблемы начинаются с переписки с незнакомцами, скачиваний и публикации личных фото.



> Личные данные: что нельзя публиковать в открытом доступе

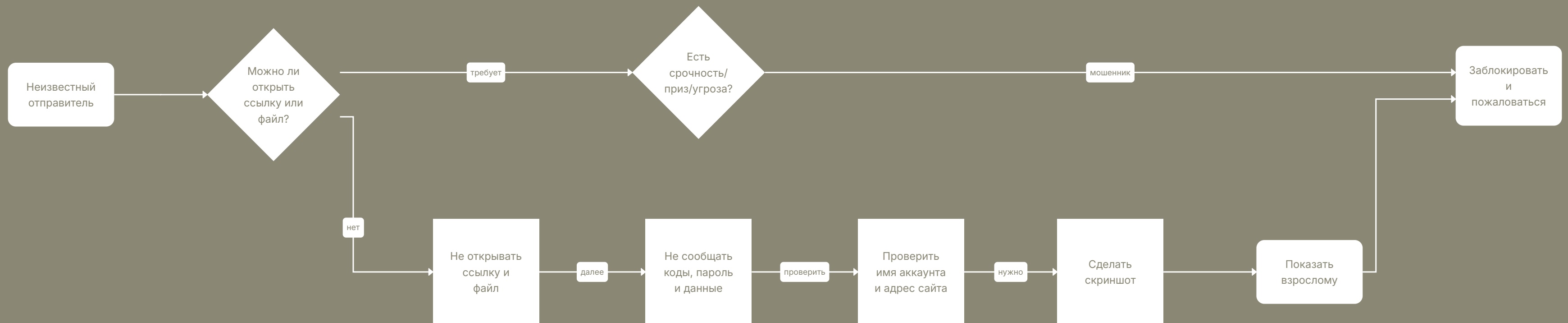
К личным данным относятся имя и фамилия, домашний адрес, номер школы и класс, телефон, пароли и коды из SMS. Даже одна деталь может стать ключом к дальнейшим действиям злоумышленника.

Опасной бывает «частичная» информация: имя + номер школы + район проживания. В таком наборе незнакомцу проще собрать о ребёнке больше сведений и выйти на контакт.

Отдельный риск создают фотографии с адресными табличками, бейджами, школьной формой и включённой геометкой. Лучше избегать таких снимков и отключать привязку по местоположению.

> Алгоритм действий при подозрительном сообщении

Порядок шагов: от проверки до блокировки и жалобы — особенно при срочности, призах и угрозах.



> Частые угрозы в сети и первые действия

Угроза	Признак	Первая реакция
Фишинг	Выманивают пароль или код	Не вводить данные, закрыть страницу
Кибербуллинг	Оскорбления, угрозы, насмешки	Сохранить переписку, прекратить контакт
Вредоносные файлы	Заражённые ссылки, архивы	Не скачивать и не запускать
Фейковые конкурсы	«Бесплатные подарки» ради данных	Проверить источник, не переходить по ссылке
Общий принцип	Срочность или давление	Чем быстрее остановить контакт, тем безопаснее

Ниже — самые распространённые виды опасности и что сделать в первые минуты, чтобы снизить риск.

Угроза обычно развивается через контакт и действие. Если быстро прекратить переписку и не выполнять просьбы злоумышленника, вероятность вреда заметно снижается.

Обобщённые правила цифровой безопасности для школьников.

> Где школьники чаще всего сталкиваются с рисками

В мессенджерах и играх проще начать личный разговор, попросить фото или код, переслать опасную ссылку.

Чаще всего проблемы возникают там, где быстро общаются и легко делятся материалами. Значит, именно там нужна особенно внимательная проверка контактов и ссылок.

Учебное обобщение типичных сценариев риска (без привязки к конкретной статистике).

> Как распознать опасного незнакомца в сети

Темп разговора и переход к личному

Опасный контакт часто начинает разговор слишком быстро и переводит тему в личные вопросы: возраст, адрес, школа. Может просить фото или видео, чтобы получить материалы и продолжить давление.

Предложения, которые нарушают границы

Тревожные сигналы — подарки за общение, просьбы скрыть переписку от родителей и предложение перейти в другой чат. Иногда человек уговаривает отправить «самое важное» прямо сейчас.



> Пароли и защита аккаунтов

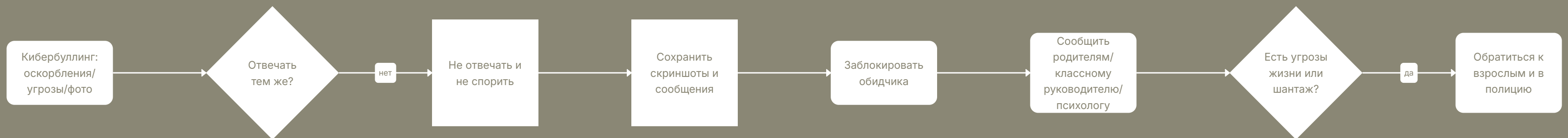
Надёжный пароль обычно содержит не менее 10–12 символов: буквы в верхнем и нижнем регистре, цифры и знаки. Это снижает шанс подбора и угадывания.

Один и тот же пароль для разных сайтов опасен: если взломают один аккаунт, пострадают и другие. Дополнительную защиту даёт двухфакторная проверка входа — код из SMS или приложение.

Пароли и коды нельзя сообщать друзьям, одноклассникам и незнакомым людям. Даже если просят «помочь войти», безопаснее отказаться и предупредить взрослого.

> Что делать при кибербуллинге

Последовательность действий: сохранить доказательства, остановить контакт, привлечь взрослых и действовать при угрозах.



> Цифровой след: что остается после публикаций

Самые заметные следы часто оставляют фотографии, скриншоты и комментарии: их легко переслать и сохранить.

Даже удалённая публикация может продолжать «жить» в пересылках и копиях. Поэтому важно думать перед тем, как написать или отправить что-то.

Учебное обобщение на основе типичных способов распространения контента в сети (без привязки к конкретной статистике).

> Правила безопасного общения в интернете

Правило	Что делать
Вежливость	Без оскорблений
Чужие материалы	Не пересылать без разрешения
Провокации	Не спорить с троллями
Грубость	Не отвечать грубостью
Информация	Проверять перед репостом
Давление	Прекратить разговор и сообщить взрослому

Чтобы переписка оставалась безопасной, важны правила поведения: вежливость, уважение границ и аккуратность с контентом. Отдельно важно прекращать контакт, если собеседник давит или запугивает.

Когда вы выбираете уважительный тон и делаете паузу перед отправкой сообщения, конфликтов и рискованных ситуаций становится меньше.

> Проверяем информацию по шагам

Шаг 2: найдите первоисточник

Ищите, откуда информация появилась сначала: сайт учреждения, пресс-релиз, оригинальное видео/пост. Если первоисточника нет — не распространяйте новость.

Шаг 4: проверьте дату и автора

Дата публикации и автор помогают понять, не устарело ли сообщение и кто несет ответственность за текст. После этого решайте: репостить или нет.

Шаг 1: насторожитесь

Громкий заголовок, эмоции и восклицательные знаки часто используют, чтобы вы не думали. Проверьте, есть ли ссылка на первоисточник и указаны ли автор и организация.

Шаг 3: сверка с источниками

Сравните утверждение минимум с 2–3 надежными сайтами. Особое внимание — совпадает ли фактура: дата, место, цифры, имена и формулировки.



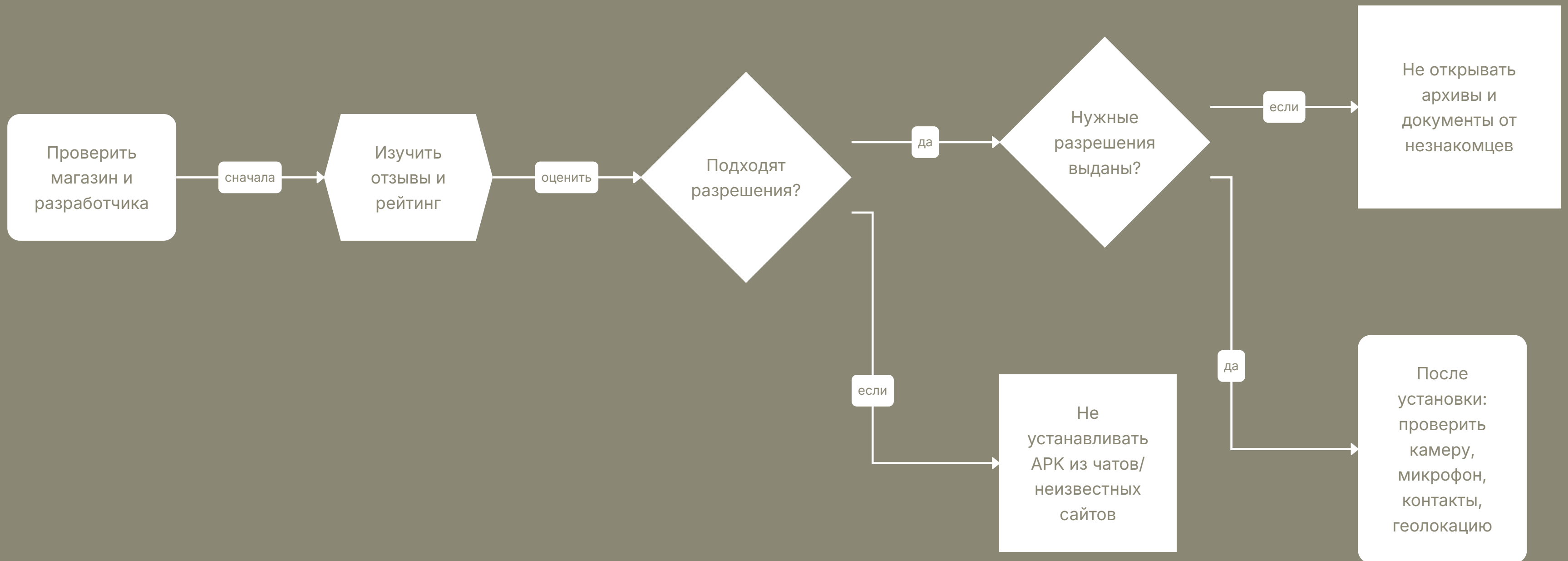
1) Бесплатные скины, монеты, призы и «секретные подарки» нередко используют как приманку для перехода на мошеннический сайт. Обычно там торопят и обещают редкую награду без условий.

2) Опасные признаки — срочность, обещание «только сейчас» и просьба ввести пароль, код или данные карты. Если вы сомневаетесь, не кликайте и сообщите взрослому.

Слишком хорошие предложения в играх и соцсетях

> Как безопасно загружать приложения и файлы

Последовательность проверки перед установкой (магазин, разработчик, разрешения, формат файлов)



> Какие разрешения приложений требуют особого внимания

Разрешения влияют на то, какую личную информацию приложение может получать. Особенно тщательно оценивайте доступ к месту и контактам, даже если приложение кажется «игровым» или «безопасным».

Чем больше разрешение связано с личной жизнью, тем выше риск. Геолокация и контакты дают много контекста о человеке и его общении.

> План действий, если в сети стало страшно или неудобно

Ситуация	Первое действие	Дальше
Угроза/шантаж	Не отвечать	Скриншот + выход из чата
Просьба фото	Сделать скриншот	Сообщить взрослому
Подозрительный звонок	Не соглашаться	Проверить информацию и прекратить контакт
Взлом аккаунта	Не продолжать пользоваться	Сменить пароль + проверить входы
Взлом аккаунта	Завершить лишние сеансы	Обратиться в службу поддержки

Если вас пугают, шантажируют, просят личные фото или предлагают опасные шаги, действуйте быстро и фиксируйте доказательства. При взломе — проверьте активные сеансы и обратитесь в поддержку.

Быстрое прекращение контакта и фиксация материалов помогают уменьшить вред и ускоряют помощь со стороны взрослых и сервиса.

Общие практики реагирования на киберриски (безопасное поведение подростков)

> Сетевой этикет: уважение в переписке и комментариях



Уважение как в школе

Здороваться, не перебивать и не переходить на личности — базовые правила. Шутка или «мем» могут задеть сильнее, чем кажется, если у людей разные чувства и контекст.



Соблюдайте границы

Не оскорбляйте и не высмеивайте ошибки. Если видите провокации, лучше промолчать и не подливать масла в конфликт. Умение остановиться снижает риск травли.



Не публикуйте чужое без согласия

Не размещайте и не пересылайте чужие фото без разрешения. Даже короткий комментарий может повлиять на человека, поэтому уважайте приватность и договоренности.



Пауза перед ответом

Если вас задели, не отвечайте грубостью. Сначала подумайте, что будет дальше: конфликт усилится или решится. Пауза помогает выбрать безопасный и корректный тон.

> Безопасность на телефоне и дома



Для защиты устройства включите блокировку экрана с PIN-кодом или отпечатком пальца, установите автоматические обновления, а также проверьте работу антивируса. Это снижает риск взлома и заражения вредоносными программами.

Сделайте резервную копию данных: фотографии, контакты и важные файлы сохранятся при потере или поломке телефона. Резервная копия помогает восстановиться без лишних переживаний и быстрее обратиться за помощью.

> Польза и риск: как выглядит баланс онлайн-активности

Интернет помогает учиться, общаться и творить, но риск растет, когда вы спешите, доверяете незнакомцам или публикуете личные данные. Секрет — проверять и не торопиться.

Риск не исчезает полностью, но им можно управлять: аккуратная переписка, внимательные ссылки и остановка перед публикацией уменьшают вероятность проблем.

Обобщенная модель соотношения пользы и рисков для учебных целей (без точных статистических данных)

> Главные выводы: безопасное поведение в сети — это привычка

Не публикуйте личные данные,
проверяйте ссылки и людей и
сразу обращайтесь к взрослым
при угрозе. Для семиклассника
важны внимательность, уважение,
аккуратность с файлами и
привычка думать перед
сообщением.