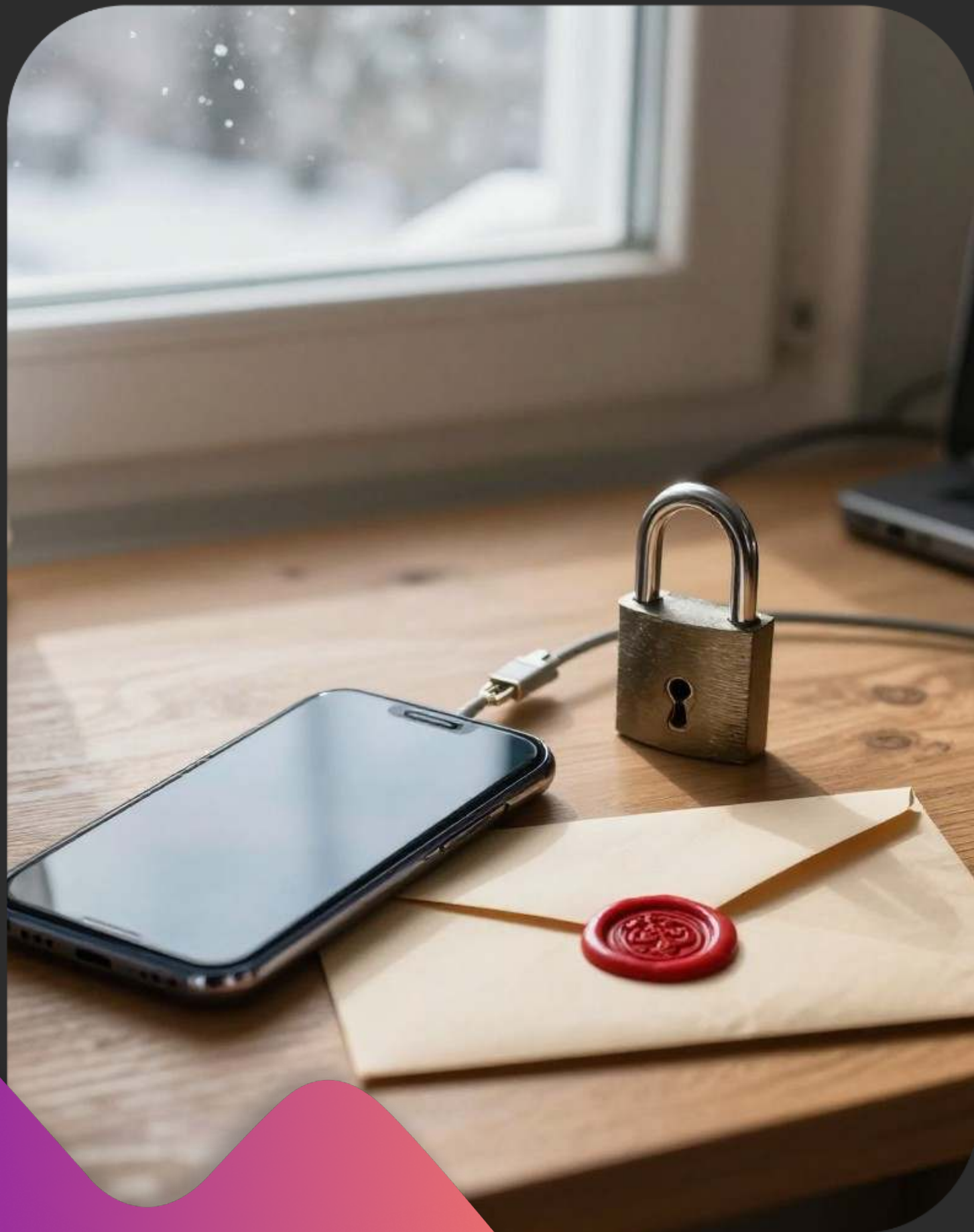


# Информационная безопасность и этика в цифровом мире

Разберём защиту личных данных,  
безопасные действия в сети и уважение к  
другим.



# Почему это важно именно вам (8 класс)

Смартфоны, мессенджеры, игры и школьные платформы стали частью дня. В переписках и чатах появляются личные фото и контакты, а ошибки ведут к взлому, утечке сообщений, буллингу и конфликтам, а иногда — к потере учебных файлов.



# Что такое информационная безопасность

Информационная безопасность — это защита данных, устройств и аккаунтов от кражи, удаления, подмены и утечки, чтобы вы могли пользоваться сервисами без лишнего риска и тревоги.

Защита информации опирается на три свойства: конфиденциальность (доступ только нужным), целостность (данные не искажены) и доступность (к ним есть законный доступ).

Ключевые угрозы — вирусы и вредоносные программы, поддельные сайты, взлом паролей, вредоносные ссылки и социальная инженерия, когда злоумышленник давит эмоциями или обещаниями.

# Основные угрозы и возможный вред

| Угроза            | Что происходит                                                            |
|-------------------|---------------------------------------------------------------------------|
| Фишинг            | Поддельное сообщение/сайт → кража пароля и доступа                        |
| Слабый пароль     | Короткий или одинаковый → взлом и доступ к переписке                      |
| Вирус             | Вредоносный файл/приложение → удаление, слежка, сбои                      |
| Публикация данных | Адрес, телефон, школа, геолокация → риск обмана и нежелательных контактов |
| Публичный Wi-Fi   | Небезопасная сеть → перехват данных при входе                             |

Школьная памятка по кибергигиене

Смотрите, как разные угрозы отражаются на аккаунтах, данных и приватности.

Одна ошибка способна одновременно нарушить приватность и привести к потере доступа к аккаунту или данным.

# Цифровой след: что остается в интернете

## Что входит в цифровой след

Цифровой след включает публикации, лайки, комментарии, фотографии, геолокацию и историю поиска. Даже удалённое сообщение может сохраниться в скриншоте, пересылке или архиве, сделанном другим человеком.

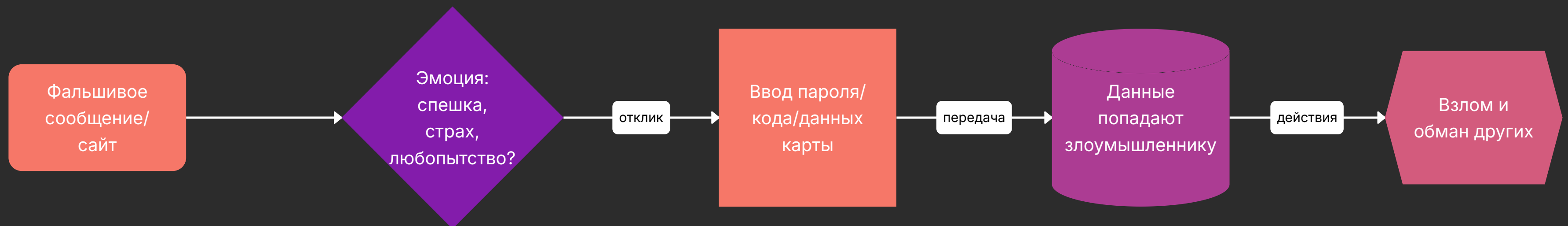
## Почему «удалил» не всегда значит «исчезло»

Цифровой след влияет на то, как вас воспринимают: в классе, в чатах и даже в будущем. Поэтому важно заранее думать, что вы пишете и публикуете — и с кем это может остаться.



# Как работает фишинг

Схема процесса (по шагам, которые повторяются в большинстве атак)



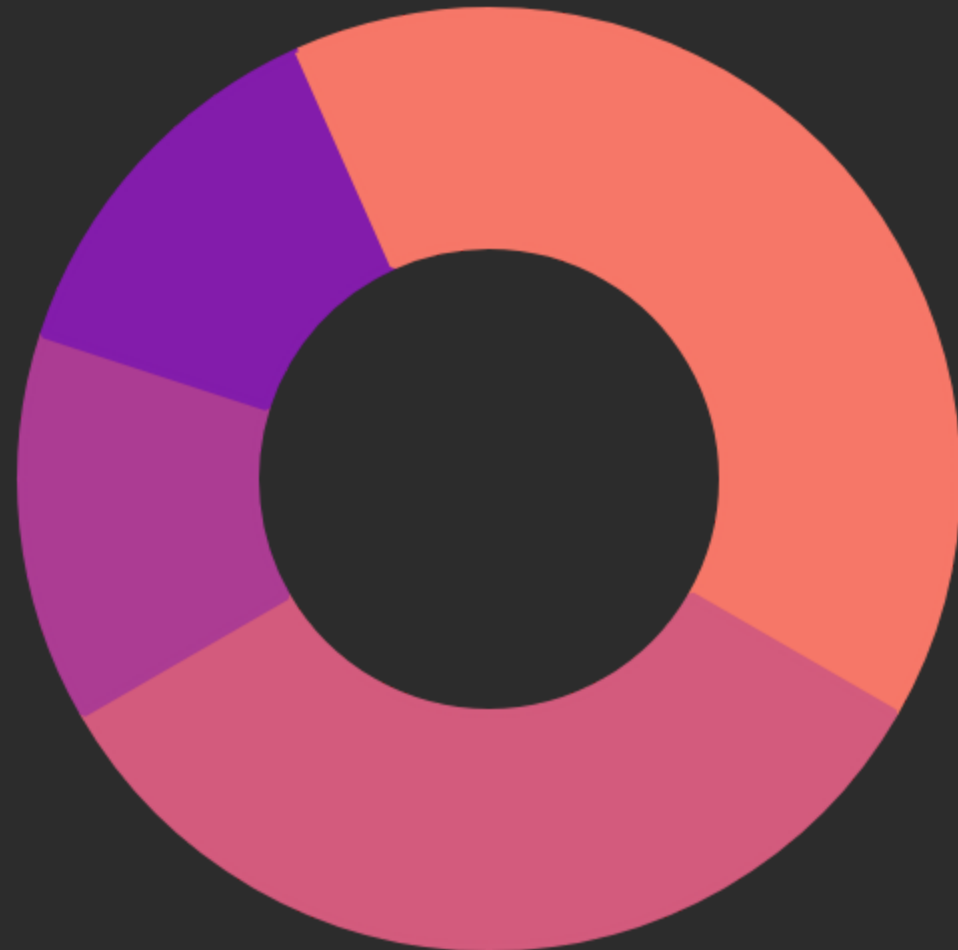
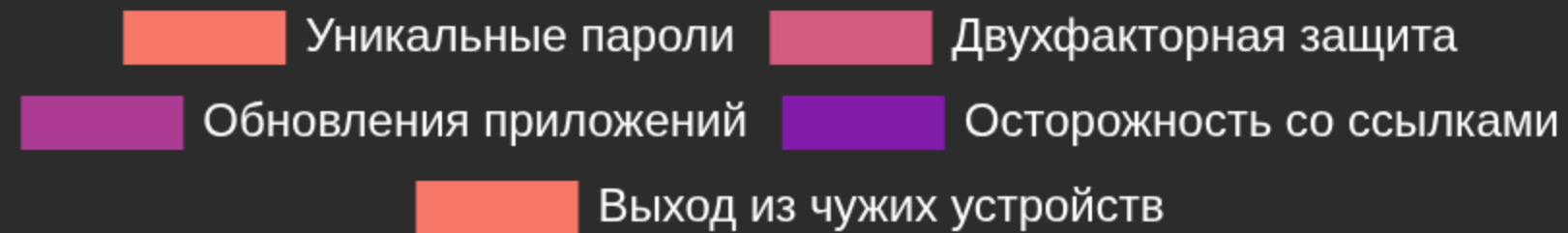
# Пароли и двухфакторная защита

Надёжный пароль — это не менее 12 символов и сочетание букв разного регистра, цифр и знаков. Такой пароль сложнее подобрать, даже если кто-то попытается угадать варианты.

Главное правило — один и тот же пароль нельзя использовать для разных сервисов. Тогда утечка из одного места не превращается в «ключ от всего», и ваши аккаунты остаются защищёнными.

Двухфакторная защита добавляет второй шаг входа: код из приложения, SMS или подтверждение на другом устройстве. Даже при утечке пароля вход будет остановлен без второго подтверждения.

# Что сильнее всего защищает аккаунт



Самую заметную роль играют два слоя защиты: уникальные пароли и двухфакторная проверка. Остальные меры снижают риск, дополняя их.

Картина показывает приоритет: сначала защищаем вход (пароль + второй фактор), затем уменьшаем вероятность ошибок с ссылками и уязвимостями.

Учебная схема кибергигиены (условные доли; точные проценты не задавались)

# Безопасное поведение в мессенджерах и играх



## Не делитесь личными данными

Незнакомым людям нельзя передавать фото документов, адрес, номер телефона, школу, пароли и коды из сообщений. Даже «друзья по рекомендации» могут оказаться мошенниками.



## Осторожно с ссылками и «бесплатным»

В играх и чатах часто обещают бесплатную валюту, редкие предметы и бонусы. Такие предложения нередко ведут на поддельные страницы и помогают обмануть игрока или украсть вход.



## Файлы и ссылки — только после проверки

Сомнительные вложения и ссылки не открывайте без проверки. Они могут содержать вредоносное ПО или подталкивать к ошибочным действиям, например к вводу данных на фальшивой странице.

# Кибербуллинг: когда сеть становится опасной

- Кибербуллинг — это оскорбления в чатах, обидные мемы, распространение слухов, публикация чужих фото без согласия и исключение из онлайн-групп. Эти действия быстро превращают общение в травлю.
- Последствия бывают серьёзными: стресс, тревога, страх заходить в сеть и снижение успеваемости. Важно поддержать того, кого обижают, и при необходимости использовать блокировку и жалобы.



# Этика общения в цифровой среде

Интернет-коммуникация держится на уважении: не выдавай чужие материалы за свои, не присваивай результаты одноклассников и не используйте их идеи без упоминания. Честность — основа доверия в чатах.

Вежливый тон и точные формулировки помогают избегать конфликтов. Если есть спор, обсуждай по сути, а не по личности: без оскорблений, угроз и унижительных комментариев, даже когда эмоции сильные.

Личные сообщения и переписка — это приватная зона. Нельзя пересылать их без согласия, обсуждать детали «за спиной» или превращать чужие слова в повод для насмешек. Уважай границы других.

# Цифровая этика: можно и нельзя

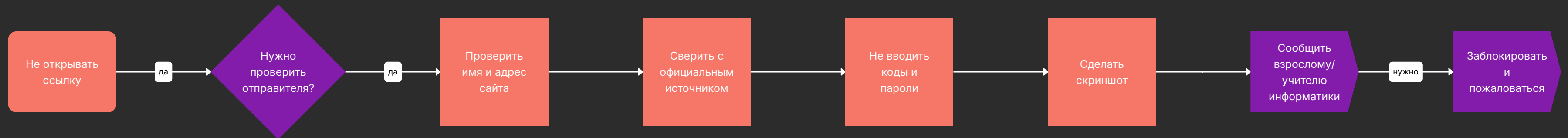
| Ситуация            | Правильно           | Ошибка                                 |
|---------------------|---------------------|----------------------------------------|
| Чужое фото          | Спросить разрешение | Выложить без согласия                  |
| Чужая презентация   | Указать автора      | Скопировать как свою                   |
| Спор в комментариях | Отвечать спокойно   | Переходить на обиды                    |
| Школьный чат        | Писать по теме      | Спамить, высмеивать, пересылать личное |

Сравните правильные и неправильные действия в типичных школьных ситуациях: публикации, учебные работы, обсуждения и школьные чаты. Главная идея — согласие, указание источников и уважение.

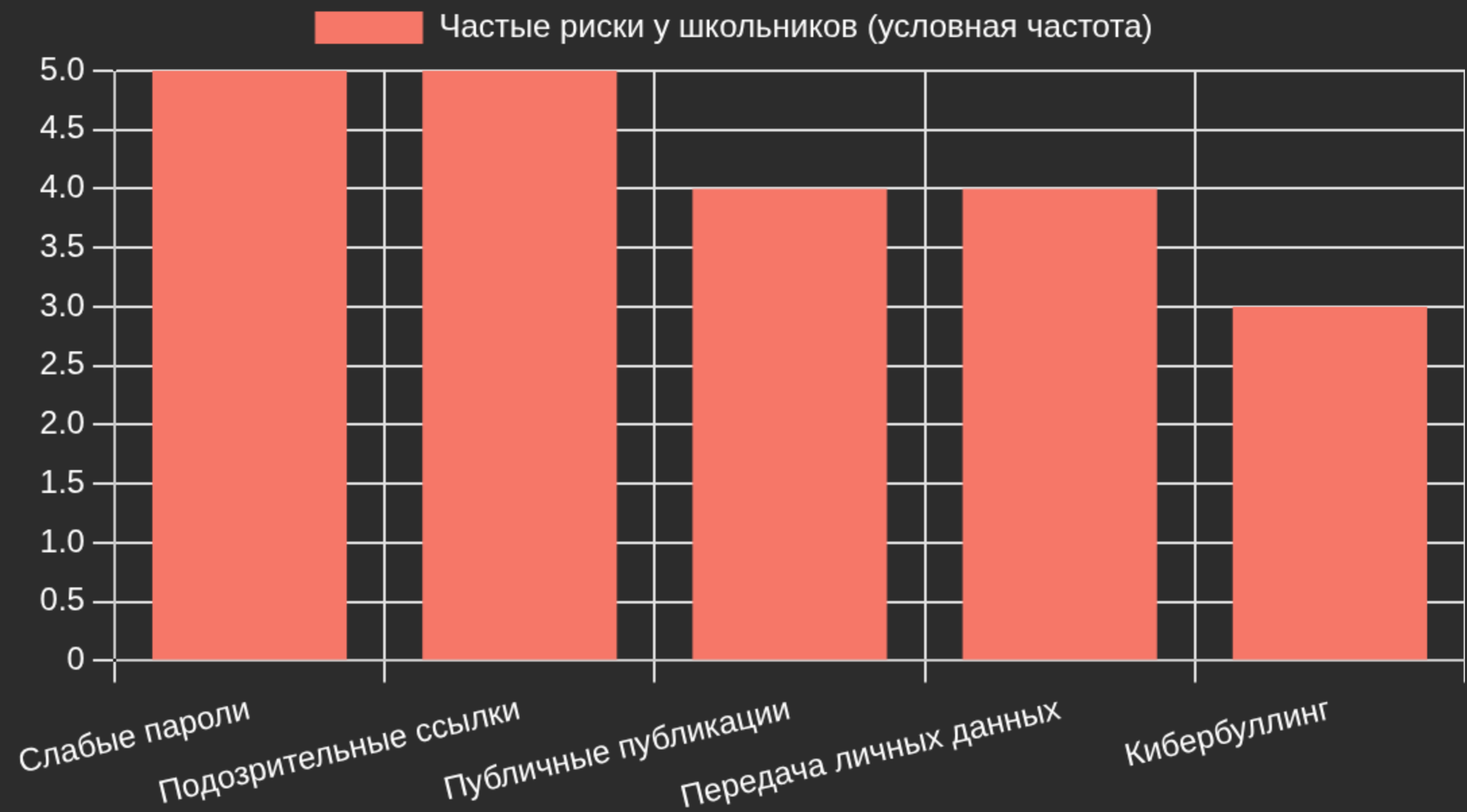
Согласие и аккуратные правила общения снижают вред: уменьшаются конфликты, риск распространения чужих данных и нарушения авторских прав.

# Как действовать при подозрительном сообщении

Пошаговый алгоритм для защиты от фишинга и мошенничества (входить в аккаунты и вводить данные нельзя).



# Какие риски чаще всего встречаются у школьников



Самые заметные проблемы связаны с входом в аккаунты: слабые пароли и переход по подозрительным ссылкам дают мошенникам прямой путь к переписке.

Даже при более редких случаях кибербуллинг и утечки информации обычно сильнее бьют по самочувствию и безопасности. Поэтому важны и профилактика, и быстрые действия.

Школьная памятка по кибергигиене (обобщение случаев), без точной статистики за год

# Авторское право и уважение к чужому труду

Любой материал — текст, изображение, музыка, видео или презентация — создан конкретным автором. Копировать без ссылки на источник или автора считается нарушением и подрывает честность учебной работы.

Допустимы собственные материалы, а также цитаты и фрагменты с указанием автора и источника. Если материал имеет открытую лицензию, его можно использовать по правилам лицензии.

Уважение к авторскому праву проявляется в мелочах: правильно указывать, откуда взяты идеи и файлы, не выдавать чужую работу за свою и не «заменять» подпись на случайную. Это формирует ответственность.

# Настройки приватности: как уменьшить риски



## **Закрой профиль и сократи личную информацию**

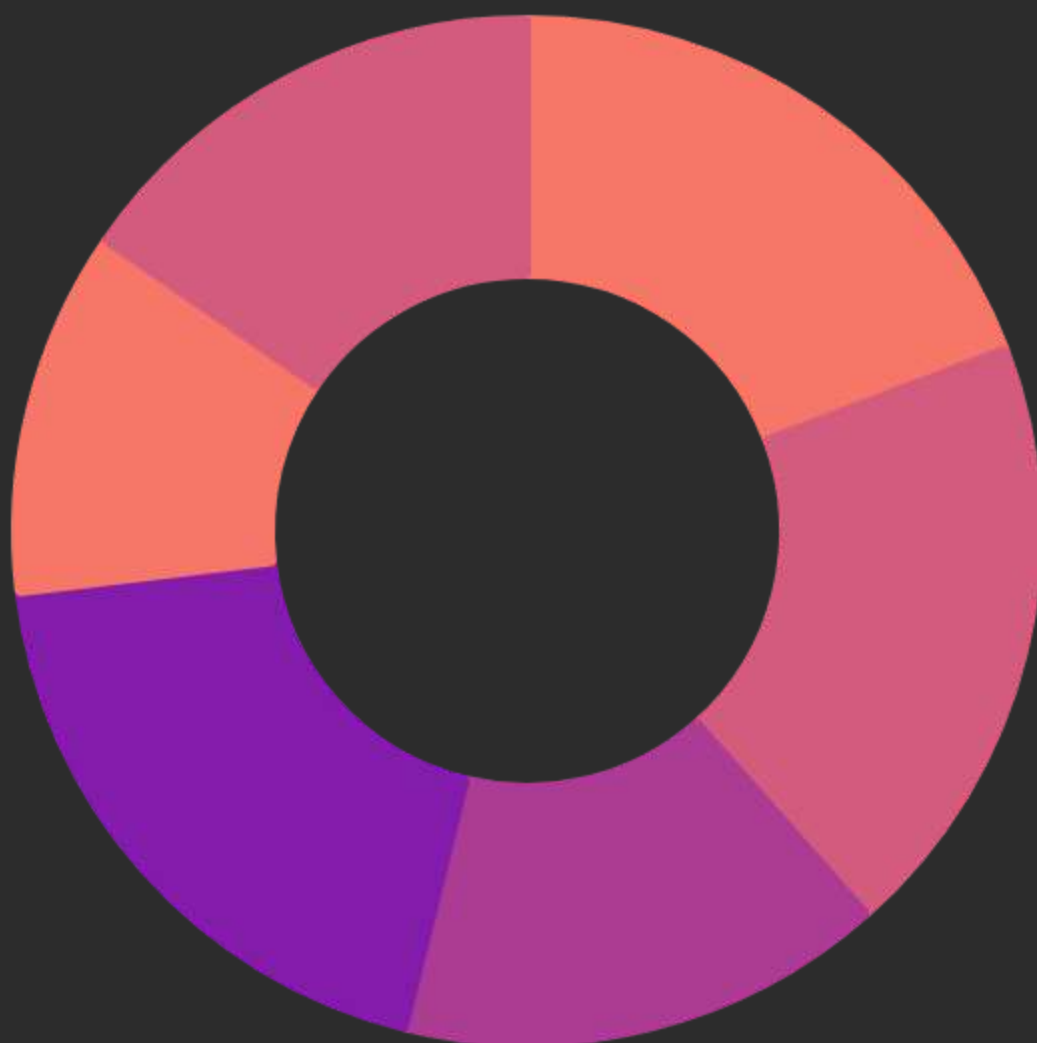
Закрытый профиль, ограничение круга друзей и скрывание геолокации уменьшают количество персональных сведений в сети. Так снижается риск нежелательных контактов и попыток обмана, опирающихся на «ваши данные».

## **Контролируй доступ приложений к данным**

Проверь разрешения приложений: какие сервисы получают доступ к камере, микрофону, контактам и местоположению. Если доступ не нужен для функции, лучше ограничить его — это уменьшает сбор лишней информации.

# Какие цифровые привычки наиболее полезны

Надёжные пароли   Регулярные обновления   Приватность  
Проверка ссылок   Уважительное общение   Резервные копии



Если объединить привычки в ежедневный ритм, риски снижаются комплексно: меньше входов «через обман», меньше утечек и легче восстановиться после ошибок или сбоев.

Наибольший эффект дают надёжные пароли, регулярные обновления и проверка ссылок. Приватность и резервные копии усиливают защиту, а уважительное общение уменьшает конфликты.

Школьные рекомендации по кибергигиене и цифровой этике (обобщение принципов), без точных измерений

# Резервные копии и обновления

## Сразу включите автоматические обновления

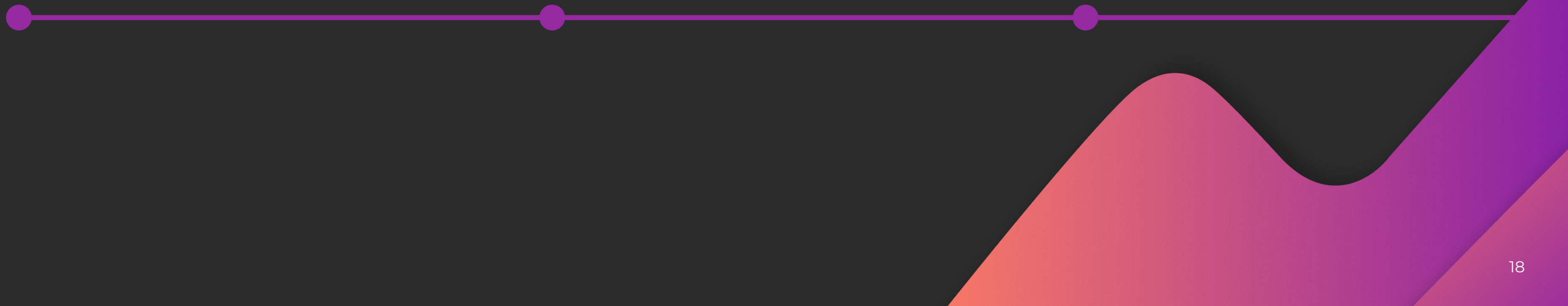
Обновления закрывают уязвимости в системе и приложениях. Так снижается риск заражения вредоносными программами и упрощается безопасность аккаунтов.

## Регулярно создавайте резервные копии учебных файлов

Копии сохраняют фото, документы и учебные материалы при поломке устройства, случайном удалении или заражении. Планы становятся спокойнее, а потери — меньше.

## Храните копии в облаке или на отдельном носителе

Надёжная практика — хранить копии в облаке или на отдельном носителе. Это помогает восстановить данные, если с основным устройством что-то случится.



# Мини-памятка безопасного поведения

| Правило                         | Зачем это нужно                |
|---------------------------------|--------------------------------|
| Не сообщать коды и пароли       | Чтобы не потерять доступ       |
| Использовать уникальные пароли  | Чтобы взлом не затронул другие |
| Проверять ссылки и отправителей | Чтобы не попасть на фишинг     |
| Уважать чужие границы           | Чтобы не нарушать приватность  |
| Делать резервные копии          | Чтобы сохранить файлы и фото   |

Школьная памятка по кибергигиене

Короткие правила, которые чаще всего предотвращают проблемы: от взлома аккаунтов до утечки личных данных и конфликтов. Используйте их как чек-лист перед действиями в сети.

Несколько простых привычек дают заметный эффект: уменьшают риск цифровых проблем и делают действия в интернете более осознанными.

# Главный вывод: безопасность и этика работают вместе

Информационная безопасность защищает данные, устройства и аккаунты, а этика — людей и их репутацию. Пароли, двухфакторная защита, приватность, внимательность к ссылкам и уважение к чужому труду создают единую грамотность для ученика 8 класса.