**ВСЕРОССИЙСКИЙ МОЛОДЁЖНЫЙ КОНКУРС ПО ПРОБЛЕМАМ КУЛЬТУРНОГО НАСЛЕДИЯ, ЭКОЛОГИИ И БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ**

# «ЮНЭКО»

---

**Направление: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ**

**Тема: «Цифровая безопасность подростков: основные интернет – угрозы и способы защиты персональных данных»**

**Соискатель: Сохрякова Александра Юрьевна**
студент ГАПОУ «Бузулукский строительный колледж»

**Научный руководитель: Добрынина Светлана Константиновна**
преподаватель специальных дисциплин, высшей категории,
знак отличия «За успехи в научно-исследовательской работе студентов»

**Место выполнения работы: ГАПОУ «Бузулукский строительный колледж» г. Бузулука Оренбургской области**

**Бузулук**

**2026**

**Аннотация**

Актуальность исследования обусловлена распространением фишинга, социальной инженерии, мошеннических сообщений, кражи учётных данных, утечек персональной информации и других цифровых угроз, с которыми пользователь может столкнуться в повседневной жизни.

Цель работы — изучение основных интернет-угроз для подростков и разработка практических рекомендаций по защите персональных данных, аккаунтов и устройств.

Для достижения поставленной цели определены следующие задачи: раскрыть понятие цифровой безопасности; рассмотреть особенности персональных данных и цифрового следа; систематизировать основные виды интернет-угроз; изучить способы защиты аккаунтов и устройств; проанализировать типичные ситуации цифровых рисков; разработать практическую памятку по безопасному поведению в сети Интернет.

В работе использованы следующие методы исследования: анализ нормативных и информационных источников, классификация и систематизация цифровых угроз, сравнение способов защиты, анализ типичных цифровых ситуаций, обобщение полученной информации и разработка практического информационного продукта.

В результате исследования выделены основные угрозы цифровой безопасности подростков, рассмотрены способы их предупреждения и определены базовые правила безопасного поведения в цифровой среде. В практической части разработана памятка «10 правил цифровой безопасности подростка», включающая рекомендации по созданию и защите паролей, использованию двухфакторной аутентификации, проверке ссылок и файлов, защите персональных данных, настройке приватности и действиям при подозрении на взлом аккаунта.

Выводы исследования показывают, что цифровая безопасность зависит не только от технических средств защиты, но и от внимательности и информационной грамотности пользователя. Знание признаков цифровых угроз и соблюдение базовых правил безопасности позволяют снизить вероятность распространённых цифровых рисков.

Практическая значимость работы заключается в возможности использования разработанной памятки подростками в повседневной цифровой среде, а также при проведении занятий по информатике, классных часов и мероприятий, посвящённых цифровой грамотности и безопасному поведению в сети Интернет.

**Содержание**

Введение ……..…….. 4
1. Теоретические основы цифровой безопасности подростков …… 7
1.1. Понятие цифровой безопасности ……..… 7
1.2. Персональные данные и цифровой след …….. 7
1.3. Основные интернет-угрозы для подростков …… 7
1.4. Социальная инженерия, фишинг и мошенничество …… 8
1.5. Угрозы в социальных сетях и мессенджерах ……...… 9
2. Основные способы защиты в цифровой среде ……..... 10
2.1. Пароли и аутентификация …….…... 10
2.2. Защита аккаунтов и устройств …… 10
2.3. Безопасное поведение при получении сообщений и ссылок …… 11
2.4. Защита персональных данных и цифрового следа ……..….. 12
2.5. Действия при подозрении на взлом или мошенничество ……..…... 12
3. Практическая часть: разработка памятки по цифровой безопасности ……... 13
3.1. Методика и критерии разработки памятки ……..….. 13
3.2. Анализ типичных цифровых ситуаций ……..…... 13
3.3. Памятка «10 правил цифровой безопасности подростка» ……..… 15
3.4. Практическая значимость исследовательской работы ……. 15
Выводы ……..…... 16
Заключение ……..… 16
Список использованных источников ……..….. 16
Приложение 1. Памятка ……..... 18
Приложение 2. Чек-лист самопроверки …….. 19
Приложение 3. Презентация …… 20

## Введение

Актуальность исследования

Современная жизнь очень тесно связана с цифровыми технологиями. Интернет используется подростками для обучения, общения, поиска информации, просмотра контента, развлечений и решения повседневных задач. Социальные сети, мессенджеры, электронная почта, онлайн-сервисы и различные приложения уже стали привычной частью жизни школьников. Но вместе с удобством цифровой среды увеличивается и количество рисков, связанных с использованием Интернета.

Одной из наиболее значимых проблем является недостаточная осведомлённость пользователей о способах защиты персональной информации. Подросток может ежедневно сталкиваться с подозрительными сообщениями, неизвестными ссылками, попытками получить пароль или код подтверждения, фальшивыми аккаунтами, мошенническими предложениями и другими видами цифровых угроз. Опасность заключается в том, что внешне такие ситуации часто выглядят обычными и не вызывают подозрений.

Особое значение имеет защита персональных данных. Имя, номер телефона, адрес электронной почты, фотографии, данные аккаунтов, сведения об учебном заведении и другая информация могут использоваться злоумышленниками для обмана, получения доступа к аккаунтам или дальнейшего распространения информации. Кроме того, публикации и фотографии, размещённые в Интернете, могут формировать цифровой след пользователя и сохраняться в сети длительное время.

Проблема цифровой безопасности становится особенно актуальной для подростков, поскольку значительная часть их общения и деятельности проходит в цифровой среде. При этом технические средства защиты сами по себе не гарантируют полной безопасности. Большое значение имеют внимательность пользователя, критическое восприятие информации и знание основных правил поведения в Интернете.

Таким образом, возникает необходимость систематизировать наиболее распространённые цифровые угрозы и определить доступные способы защиты, которые могут применяться подростками в повседневной жизни.

Правовые основы защиты информации в Российской Федерации определяются, в частности, Федеральным законом № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Вопросы обработки персональных данных регулируются Федеральным законом № 152-ФЗ «О персональных данных». Эти нормы показывают, что защита информации является не только технической, но и правовой задачей.

Проблема исследования

Проблема исследования заключается в противоречии между активным и практически ежедневным использованием подростками цифровых технологий, социальных сетей, мессенджеров и различных интернет-сервисов и недостаточным уровнем их осведомлённости о существующих интернет-угрозах и способах защиты личной информации. Подростки регулярно создают аккаунты, используют пароли, публикуют фотографии и другие персональные сведения, общаются с незнакомыми людьми и переходят по различным интернет-ссылкам, однако не всегда осознают возможные последствия неосторожного поведения в цифровой среде. Это может привести к утечке персональных данных, взлому аккаунтов, распространению личной информации, мошенничеству, заражению устройств вредоносными программами и другим

угрозам. В связи с этим возникает необходимость изучения основных видов интернет-угроз, с которыми могут столкнуться подростки, а также формирования у них практических навыков безопасного поведения в интернете и защиты своих персональных данных, аккаунтов и цифровых устройств.

Цель исследования

Целью исследования является комплексное изучение основных интернет-угроз, с которыми подростки могут столкнуться при использовании социальных сетей, мессенджеров, электронной почты и других цифровых сервисов, выявление наиболее распространённых способов получения и неправомерного использования персональных данных, а также определение эффективных и доступных способов защиты аккаунтов, устройств и личной информации. На основе проведённого исследования предполагается разработать практические рекомендации и памятку, которые помогут подросткам распознавать потенциально опасные ситуации, соблюдать правила безопасного поведения в сети Интернет и снижать риск столкновения с распространёнными цифровыми угрозами.

Задачи исследования

Для достижения поставленной цели необходимо решить следующие задачи:
- раскрыть понятие цифровой безопасности;
- рассмотреть понятие персональных данных и цифрового следа;
- определить основные виды интернет-угроз, актуальные для подростков;
- рассмотреть особенности фишинга, социальной инженерии и интернет-мошенничества;
- изучить основные способы защиты аккаунтов и цифровых устройств;
- определить правила безопасного поведения при получении подозрительных сообщений, ссылок и файлов;
- проанализировать типичные ситуации, связанные с цифровыми рисками;
- разработать практическую памятку «10 правил цифровой безопасности подростка»;
- определить практическую значимость разработанных рекомендаций.

Объект исследования

Объектом исследования является цифровая безопасность пользователей в сети Интернет.

Предмет исследования

Предметом исследования являются основные интернет-угрозы для подростков и способы защиты персональных данных, аккаунтов и цифровых устройств.

Гипотеза исследования

Предполагается, что систематизация основных интернет-угроз и распространение понятных правил цифровой безопасности позволит повысить осведомлённость подростков и снизить вероятность совершения распространённых ошибок при использовании Интернета.

Методы исследования

В работе использованы следующие методы исследования:
- анализ информационных и нормативных источников;
- изучение и обобщение материалов по вопросам цифровой безопасности;

- классификация основных видов интернет-угроз;
- сравнение способов защиты персональных данных и аккаунтов;
- анализ типичных ситуаций цифрового риска;
- систематизация полученной информации;
- разработка практического информационного продукта.

Использование указанных методов позволяет рассмотреть проблему с теоретической и практической сторон, выделить наиболее распространённые угрозы и сформулировать доступные рекомендации по безопасному поведению в цифровой среде.

Практическая значимость исследования

Практическая значимость работы заключается в создании информационного материала, который может использоваться подростками в повседневной жизни для проверки собственных навыков цифровой безопасности.

В рамках практической части разработана памятка «10 правил цифровой безопасности подростка». В ней представлены основные рекомендации по созданию и хранению надёжных паролей, использованию двухфакторной аутентификации, проверке ссылок и файлов, защите персональных данных, настройке приватности аккаунтов и действиям при подозрении на взлом.

Разработанные материалы могут применяться не только самими подростками, но и в образовательной среде: на уроках информатики, классных часах, тематических мероприятиях и занятиях по цифровой грамотности. Памятка также может использоваться как краткая инструкция для повторения основных правил безопасного поведения в Интернете.

Научная и практическая новизна

Новизна работы заключается в систематизации основных цифровых угроз с учётом типичных ситуаций, с которыми подросток может столкнуться при использовании социальных сетей, мессенджеров и других интернет-сервисов.

В отличие от простого перечисления правил безопасности, в работе рассматривается связь между конкретной цифровой ситуацией, возможной угрозой и способом защиты. На основе этого подхода разработана компактная памятка, позволяющая применять полученные знания непосредственно в повседневной цифровой среде.

Таким образом, работа объединяет теоретическое рассмотрение проблемы цифровой безопасности и практическую разработку рекомендаций, ориентированных на подростков. Результатом исследования становится не только систематизация информации об интернет-угрозах, но и создание понятного инструмента для формирования более безопасного поведения в сети Интернет.

# 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ЦИФРОВОЙ БЕЗОПАСНОСТИ ПОДРОСТКОВ

## 1.1. Понятие цифровой безопасности

Цифровую безопасность можно определить, как совокупность знаний, правил, технических средств и моделей поведения, которые позволяют человеку снижать риски при использовании цифровых устройств, сервисов и сетей. Для пользователя это означает: посторонние не должны получать доступ к личным данным; данные не должны незаметно изменяться или уничтожаться; человек должен сохранять контроль над своими аккаунтами и устройствами.

Для подростка цифровая безопасность имеет несколько уровней. Первый — технический: обновления, блокировка устройства, резервное копирование. Второй — учётные записи: уникальные пароли, многофакторная аутентификация, контроль активных сеансов. Третий — информационный: умение отличать достоверное сообщение от подозрительного. Четвёртый — коммуникативный: понимание границ общения, приватности и правил обращения за помощью.

Рекомендации CISA для обычных пользователей сводятся к нескольким базовым действиям: использовать сильные и уникальные пароли, включать многофакторную аутентификацию, распознавать фишинг и своевременно обновлять программное обеспечение [8; 9]. Эти меры не устраняют все угрозы, но создают несколько уровней защиты.

Цифровая безопасность не означает отказ от интернета. Её задача — сделать использование цифровой среды осознанным. Пользователю важнее сформировать устойчивые привычки: не торопиться, проверять источник, не передавать секретные данные и обращаться за помощью, если ситуация вызывает сомнения.

## 1.2. Персональные данные и цифровой след

В российском законодательстве персональные данные — это любая информация, относящаяся к прямо или косвенно определённому, или определяемому физическому лицу [1]. Это шире, чем паспортные данные: в зависимости от ситуации значение могут иметь имя, номер телефона, электронная почта, фотография, сведения об аккаунте и местоположении.

Цифровой след — совокупность сведений, которые возникают в результате действий человека в цифровой среде: публикации, комментарии, реакции, сведения профиля и иные элементы онлайн-активности. Часть следа создаётся пользователем, часть формируется автоматически сервисами.

Перед публикацией полезно задать три вопроса: кому это будет доступно; может ли информация навредить мне или другому человеку; согласен ли я с тем, что она останется частью моего цифрового образа? UNICEF подчёркивает значение права детей на приватность и необходимость защиты персональной информации [7].

## 1.3. Основные интернет-угрозы для подростков

Угрозы можно классифицировать по тому, на что направлено воздействие: на данные, аккаунт, устройство, деньги, репутацию или безопасность человека. Одни угрозы преимущественно технические, другие используют обман и социальное воздействие.

Угрозы могут сочетаться. Открытая фотография способна раскрыть имя, место учёбы или круг общения, а затем эти сведения могут использоваться для более убедительного сообщения. Поэтому защита начинается ещё на этапе публикации информации.

Отдельную группу составляют угрозы, связанные с искусственным интеллектом. Современные инструменты позволяют создавать убедительные тексты, изображения и имитации

голоса. Минпросвещения России уже отмечало необходимость учить школьников отличать поддельные голоса и проверять информацию [5]. Поэтому одного внешнего признака недостаточно: важны контекст и независимая проверка.

Таблица № 1

| Угроза | Что происходит | Основной риск | Базовая защита |
|---|---|---|---|
| Фишинг | Поддельный сайт, письмо или ссылка | Кража данных | Проверять источник и адрес; не использовать подозрительную ссылку |
| Социальная инженерия | Пользователя убеждают самому выполнить действие | Потеря контроля или денег | Не действовать под давлением; проверить другим каналом |
| Вредоносное ПО | На устройство попадает нежелательная программа | Кража данных, сбой | Обновления; осторожность с файлами и приложениями |
| Захват аккаунта | Посторонний получает доступ | Потеря данных и аккаунта | Уникальный пароль, MFA, контроль сеансов |
| Кибербуллинг | Травля через цифровые сервисы | Репутационный и эмоциональный вред | Блокировка, жалоба, доказательства, помощь взрослого |
| Поддельный профиль | Человек выдаёт себя за другого | Обман и выманивание сведений | Проверка личности |
| Утечка данных | Личная информация становится доступной | Мошенничество, нарушение приватности | Минимизация публикаций, настройки приватности |
| Манипулятивный контент | Пользователя подталкивают к реакции | Импульсивное решение | Пауза и проверка нескольких источников |

### 1.4. Социальная инженерия, фишинг и мошенничество

Социальная инженерия — воздействие на человека с целью побудить его раскрыть информацию или совершить нужное злоумышленнику действие. В отличие от чисто технической атаки здесь объектом воздействия становится человеческое решение. Банк России рассматривает социальную инженерию как значимый инструмент мошенничества и отдельно описывает фишинг и схемы, в которых человека убеждают самостоятельно передать сведения [2; 3].

Фишинг — распространённый пример такого подхода. Пользователю могут отправить письмо

или сообщение, внешне напоминающее официальный сервис. Целью может быть получение логина, пароля, кода или другой информации. При этом фишинговое сообщение не обязательно выглядит очевидно поддельным: оно может быть грамотно оформлено и персонализировано.
Типичные психологические приёмы:
- срочность: «сделайте это сейчас»;
- страх: «обнаружена подозрительная активность»;
- авторитет: сообщение якобы от организации или службы поддержки;
- выгода: обещание подарка, скидки или выигрыша;
- любопытство: ссылка с провокационной темой;
- социальное давление: просьба «помочь другу» или выполнить поручение знакомого аккаунта.

Главный защитный принцип — не принимать решение в условиях давления. Если сообщение требует срочности, полезно остановиться и проверить его другим каналом. Если знакомый аккаунт просит деньги, нужно связаться с человеком отдельно; если организация требует входа, лучше самостоятельно открыть официальный сайт или приложение.

Устойчивость к мошенничеству состоит не в знании всех схем, а в распознавании общей структуры: неожиданный контакт → эмоциональное давление → просьба о действии → попытка получить данные или контроль.

### 1.5. Угрозы в социальных сетях и мессенджерах

Социальные сети и мессенджеры создают удобную среду общения, но одновременно увеличивают количество контактов с незнакомыми людьми и объём информации, которую пользователь публикует. Риск возникает не из-за самого общения, а из-за отсутствия границ приватности и проверки собеседника.

Одна из проблем — поддельные аккаунты. Профиль может использовать имя, фотографию и сведения другого человека. Поэтому знакомое имя или фотография ещё не подтверждают личность. Особенно осторожно следует относиться к неожиданным просьбам о деньгах, кодах, документах или переходе по ссылке.

Кибербуллинг — травля с использованием цифровых технологий; она может происходить в социальных сетях, мессенджерах, игровых сервисах и на мобильных устройствах [10]. Важная особенность — цифровой след: сообщения и публикации могут сохраняться и использоваться как доказательства. UNICEF рекомендует фиксировать происходящее, сохранять скриншоты и обращаться за помощью [11].

При травле не следует пытаться решать ситуацию ответной агрессией. Практически полезнее сохранить подтверждения, использовать блокировку и жалобы, а также обратиться к взрослому. Отдельную опасность представляет публикация сведений о местоположении: на фотографии могут быть видны школа, адрес, маршрут или другие детали.

Безопасное использование социальных сетей строится на трёх принципах: минимизация лишней информации, проверка личности и уважительное взаимодействие. Если ситуация становится угрожающей, задача подростка — сохранить безопасность и обратиться за помощью.

## 2. ОСНОВНЫЕ СПОСОБЫ ЗАЩИТЫ В ЦИФРОВОЙ СРЕДЕ

### 2.1. Пароли и аутентификация

Пароль остаётся одним из основных элементов защиты аккаунта. Наиболее безопасный подход — длинные, случайные и уникальные пароли, не повторяющиеся в разных сервисах. CISA рекомендует сочетать сильные пароли с менеджером паролей, который помогает создавать и хранить уникальные комбинации [8; 12].

Повторное использование пароля создаёт цепной риск. Если пароль становится известен из-за утечки одного сервиса, его могут попробовать на других. Поэтому особенно важно защищать отдельными паролями электронную почту и другие аккаунты, через которые можно восстановить доступ.

Второй уровень — многофакторная аутентификация (MFA). Она требует не только пароль, но и дополнительное подтверждение личности. CISA отмечает, что MFA повышает защищённость аккаунта даже в ситуации, когда пароль был взят [9].

Таблица № 2

| Привычка | Почему это важно |
|---|---|
| Один аккаунт — один уникальный пароль | Снижает риск цепного взлома при утечке данных. |
| Не использовать дату рождения, имя и простые комбинации | Такие сведения могут быть известны из профиля. |
| Включить MFA | Добавляет второй уровень проверки личности. |
| Не сообщать коды | Код является частью подтверждения входа. |
| Проверять уведомления о новых входах | Помогает заметить подозрительную активность. |

### 2.2. Защита аккаунтов и устройств

Безопасность аккаунта зависит не только от пароля. Необходимо контролировать активные сеансы, устройства, способы восстановления доступа и уведомления о входе. Если сервис сообщает о неизвестном устройстве, следует проверить историю входов и при необходимости завершить подозрительный сеанс.

Смартфон или компьютер содержит фотографии, переписку, документы и доступ к аккаунтам. Поэтому следует использовать блокировку экрана, своевременно устанавливать обновления и делать резервные копии важных данных. CISA подчёркивает, что обновления исправляют уязвимости, поэтому откладывать их без причины не стоит [8].

Приложения желательно устанавливать из доверенных источников и проверять разрешения. Если простому приложению требуется доступ к большому объёму информации, нужно оценить, действительно ли это необходимо.

Минимальный набор защиты устройства:

- блокировка экрана;

- своевременные обновления;
- установка приложений из доверенных источников;
- проверка разрешений приложений;
- резервное копирование важных данных;
- осторожность при передаче устройства другим людям.

Чем больше ценной информации хранится на устройстве, тем важнее защищать доступ к нему. Удобство и безопасность нужно сочетать: например, сохранение паролей допустимо только при надёжной блокировке самого устройства.

### 2.3. Безопасное поведение при получении сообщений и ссылок

Самая полезная привычка при неожиданном сообщении — сделать паузу. Нужно проверить отправителя, содержание, причину обращения и действие, которое требуется. CISA рекомендует осторожно относиться к сообщениям с неожиданным запросом персональной информации и не открывать подозрительные ссылки или вложения [8].

Алгоритм «СТОП»

С — стоп: не переходить по ссылке и не отвечать сразу.

Т — требование: понять, чего хотят — пароль, код, деньги, файл или фотографию.

О — оценка: проверить отправителя, адрес сайта, контекст и признаки срочности.

П — проверка: найти независимый способ связаться с настоящей организацией или человеком.

Таблица № 3

| Признак | Вопрос для проверки |
|---|---|
| Срочность | Почему я должен сделать это прямо сейчас? |
| Неожиданный контакт | Ждал ли я вообще такого сообщения? |
| Просьба о секрете | Почему меня просят никому не говорить? |
| Непривычная манера общения | Может ли аккаунт быть поддельным или взломанным? |
| Сильные эмоции | Не пытаются ли вызвать страх, жадность или любопытство? |
| Запрос кода/пароля | Должен ли я вообще кому-то это сообщать? |
| Ссылка | Куда она действительно ведёт? |

Главный принцип: если сообщение заставляет торопиться, это дополнительная причина замедлиться. Проверка обычно занимает меньше времени, чем исправление последствий.

### 2.4. Защита персональных данных и цифрового следа

Защита персональных данных начинается с принципа минимизации: публиковать и сообщать только то, что действительно необходимо. Перед публикацией фотографии стоит проверить фон, геометки, документы, адреса и другие детали. В профиле следует ограничивать доступ к информации, которая не нужна незнакомым людям.

UNICEF подчёркивает, что фотографии, сообщения и другие действия в интернете формируют цифровой след, поэтому важно заранее думать о том, какую информацию человек оставляет о себе [6; 7]. Важно учитывать, что даже обычная информация о человеке может со временем составить достаточно подробную картину его жизни. Например, по публикациям можно узнать, где человек учится, где бывает, с кем общается, когда уезжает из дома и чем занимается в свободное время. Поэтому не стоит размещать в открытом доступе слишком много подробностей о своей повседневной жизни.

Полезно время от времени проверять свои аккаунты и удалять то, чем уже не хочется делиться. Также стоит просматривать список друзей и подписчиков, настройки приватности и разрешения, которые были предоставлены приложениям. Это помогает понять, кто имеет доступ к информации и не осталась ли какая-либо ненужная информация открытой.

Следует обращать внимание и на фотографии. На заднем плане иногда могут случайно оказаться документы, адреса, номера телефонов, пропуска, экран компьютера или другие личные сведения. Перед публикацией фотографии желательно посмотреть на неё не только с точки зрения самого изображения, но и проверить, нет ли на ней информации, которую не должны видеть посторонние люди. Таким образом, защита цифрового следа должна быть постоянной. Недостаточно один раз настроить приватность аккаунта — необходимо периодически проверять, какую информацию о себе человек оставляет в интернете и кому она доступна.

### 2.5. Действия при подозрении на взлом или мошенничество

Если пользователь заметил подозрительный вход или понял, что сообщил данные мошеннику, главное — не продолжать взаимодействие с источником угрозы.

Общий порядок действий:

- прекратить подозрительный диалог и не сообщать дополнительные сведения;
- изменить пароль с безопасного устройства, если есть основания считать его известным постороннему;
- завершить неизвестные активные сеансы и проверить восстановление доступа;
- включить MFA;
- сохранить сообщения, уведомления, адреса страниц и время события;
- сообщить взрослому, если ситуация связана с угрозами, травлей или взломом;
- при финансовом риске — как можно быстрее связаться с банком через официальный канал.

Важно не стыдить и не винить человека за ошибку. Цель реагирования — остановить последствия и восстановить контроль. Скрывание проблемы обычно затрудняет помощь.

После того как доступ к аккаунту удалось восстановить, важно проверить, не изменил ли кто-нибудь настройки безопасности. Нужно посмотреть, какие номер телефона и электронная почта указаны для восстановления, какие устройства подключены к аккаунту и какие приложения имеют к нему доступ. Если появились неизвестные устройства или подключения, их следует удалить. Также стоит проверить последние действия в аккаунте.

Например, могли быть отправлены сообщения, опубликованы записи или изменены настройки без ведома владельца. Если такое произошло, необходимо убедиться, что посторонний

человек больше не имеет доступа к аккаунту.

Если с взломанного аккаунта были отправлены подозрительные сообщения знакомым, желательно предупредить их об этом. Это поможет избежать ситуации, когда кто-то поверит мошеннику, потому что сообщение пришло с аккаунта знакомого человека. Полезно заранее знать, как восстановить доступ к своим основным аккаунтам. Лучше пользоваться только официальной помощью самого сервиса, а не случайными сайтами и людьми, которые предлагают «вернуть аккаунт» за деньги или просят предоставить пароль и коды подтверждения. После произошедшего стоит разобраться, из-за чего возникла проблема. Причиной могла стать слабая или повторяющаяся комбинация паролей, переход по подозрительной ссылке, установка неизвестного приложения или передача кому-либо кода подтверждения. Понимание причины помогает избежать такой ситуации в дальнейшем.

## 3. ПРАКТИЧЕСКАЯ ЧАСТЬ: РАЗРАБОТКА ПАМЯТКИ ПО ЦИФРОВОЙ БЕЗОПАСНОСТИ

### 3.1. Методика и критерии разработки памятки

Практический продукт разработан на основе анализа рекомендаций Банка России, Минпросвещения России, UNICEF и CISA [2; 4; 6; 8]. Учитывалось, что подростку нужна не энциклопедия терминов, а короткий алгоритм, который можно вспомнить в момент получения подозрительного сообщения.

Использованы четыре критерия. Первый — распространённость ситуации. Второй — понятность. Третий — практичность: каждое правило должно приводить к конкретному действию. Четвёртый — универсальность: правило должно работать независимо от конкретного приложения.

Таблица № 4

| Критерий | Вопрос | Результат |
|---|---|---|
| Понятность | Поймёт ли подросток правило без специальных знаний? | Короткая формулировка. |
| Практичность | Что именно нужно сделать? | У каждого правила есть действие. |
| Универсальность | Работает ли правило в разных сервисах? | Нет привязки к одному приложению. |
| Проверяемость | Можно ли проверить выполнение? | Использование чек-листа. |
| Безопасность | Не создаёт ли совет дополнительного риска? | Нет взаимодействия с реальными злоумышленниками. |

В основу памятки положен принцип «сначала остановись, потом проверь». Он выбран потому, что многие схемы социальной инженерии используют спешку и эмоциональное давление. Памятка не обещает абсолютной защиты; её задача — снизить вероятность импульсивного решения.

**3.2. Анализ типичных цифровых ситуаций**

Для проверки применимости подхода смоделированы типичные цифровые ситуации. Каждая анализируется по четырём шагам: признак угрозы → возможный риск → ошибочное действие → безопасный алгоритм. Это учебные модели, а не реальные истории участников проекта.

1. «Срочное сообщение от сервиса»
Ситуация. Пользователь получает уведомление о якобы блокировке аккаунта и ссылку.
Признаки риска. Срочность, страх, ссылка.
Возможный риск. Ввод данных на поддельной странице.
Безопасное действие. Не переходить; самостоятельно открыть официальный сервис и проверить состояние аккаунта.

2. «Код, который нужно назвать»
Ситуация. Собеседник утверждает, что код нужен для отмены операции.
Признаки риска. Просьба сообщить секретный код.
Возможный риск. Код может использоваться для подтверждения входа.
Безопасное действие. Не сообщать; прекратить разговор; обратиться в официальный сервис.

3. «Сообщение от знакомого аккаунта»
Ситуация. Друг просит срочно перевести деньги или отправить код.
Признаки риска. Необычная манера и срочность.
Возможный риск. Аккаунт мог быть взломан.
Безопасное действие. Связаться с человеком другим способом.

4. «Ссылка на подарок»
Ситуация. Обещают бонус, если пользователь введёт данные.
Признаки риска. Слишком выгодное предложение и форма сбора данных.
Возможный риск. Передача логина, пароля или контактов.
Безопасное действие. Не вводить данные; проверить предложение на официальном ресурсе.

5. «Фото документа»
Ситуация. Незнакомец просит фотографию паспорта или другого документа.
Признаки риска. Запрос чувствительной информации.
Возможный риск. Утечка персональных данных.
Безопасное действие. Не отправлять; обсудить ситуацию со взрослым.

6. «Публикация с лишними деталями»
Ситуация. На фото видны школа, адрес или маршрут.
Признаки риска. Непреднамеренное раскрытие.
Возможный риск. Посторонний получает лишние сведения.
Безопасное действие. Проверить фон, геометки и аудиторию.

7. «Онлайн-травля»
Ситуация. В чате регулярно публикуют оскорбления или неприятные материалы.
Признаки риска. Повторяемость и давление.
Возможный риск. Распространение материалов и усиление конфликта.

Безопасное действие. Сохранить доказательства, заблокировать, пожаловаться, обратиться к взрослому.

8. «Подозрительное приложение»
Ситуация. Предлагают скачать приложение из неизвестного источника.
Признаки риска. Неофициальный источник.
Возможный риск. Вредоносное ПО или лишние разрешения.
Безопасное действие. Не устанавливать; искать приложение через доверенный источник.

Анализ показывает общую структуру большинства ситуаций: пользователя побуждают действовать быстрее, чем он успевает проверить информацию. Поэтому универсальный навык — перейти от эмоциональной реакции к проверке.

**3.3. Памятка «10 правил цифровой безопасности подростка»**

1. Не спеши — Если тебя торопят — остановись и проверь.
2. Не сообщай секретные данные — Пароли и коды подтверждения нельзя передавать другим людям.
3. Проверяй ссылки — Не переходи по неожиданной ссылке; открой сервис самостоятельно.
4. Используй уникальные пароли — Один важный аккаунт — один отдельный пароль.
5. Включай MFA — Дополнительное подтверждение входа снижает риск захвата аккаунта.
6. Обновляй устройства — Устанавливай обновления системы и приложений.
7. Думай перед публикацией — Проверь фон, геометки и аудиторию.
8. Проверяй собеседника — Необычную просьбу знакомого подтверждай другим способом.
9. Сохраняй доказательства — При травле, угрозах или мошенничестве не удаляй сообщения сразу.
10. Проси помощи — При угрозе, взломе или мошенничестве обратись к взрослому и в официальный сервис.

Формула памятки: «Остановись → Проверь → Не передавай секретное → Обратись за помощью». Она не заменяет правила конкретного сервиса, но помогает выбрать безопасную первую реакцию.

**3.4. Практическая значимость исследовательской работы**

Практическая ценность исследовательской работы заключается в переводе теоретических рекомендаций в формат, который легко применять в повседневной жизни. Памятка может использоваться подростками самостоятельно, а также педагогами и родителями.
Возможные форматы применения:
- раздаточный материал на классном часе;
- основа для занятия по информатике или ОБЗР;
- памятка перед началом учебного года;
- материал для обсуждения с родителями;
- чек-лист для самостоятельной проверки настроек аккаунтов;
- основа для учебного разбора фишинговых сценариев без взаимодействия с реальными подозрительными ресурсами.

Работа соответствует направлению информационных технологий, поскольку рассматривает цифровую среду как систему взаимодействия человека с данными, устройствами и информацией. Практическая часть ориентирована на цифровую грамотность и профилактику рисков.

На основе продукта можно создать интерактивный тест, карточки с ситуациями или плакат. При этом учебные сценарии должны быть безопасными: участник не вводит реальные пароли и не передаёт личные данные.

**Вывод исследовательской работы**

Исследовательская работа не ставила целью измерить статистическую распространённость угроз среди конкретной студенческой группы. В работе не использовались вымышленные опросы или придуманные проценты. Практический результат основан на анализе открытых рекомендаций и моделировании типичных ситуаций.

## ЗАКЛЮЧЕНИЕ

В ходе исследования рассмотрена проблема цифровой безопасности подростков и разработан практический инструмент для снижения рисков. Анализ показал, что безопасность включает не только технические меры, но и поведение пользователя: работу с паролями, проверку сообщений и ссылок, защиту персональных данных, контроль цифрового следа и умение обращаться за помощью.

Задачи исследовательской работы решены последовательно. Раскрыто понятие цифровой безопасности; рассмотрены персональные данные и цифровой след; систематизированы угрозы; изучены социальная инженерия и фишинг; проанализированы способы защиты аккаунтов и устройств; разработаны критерии оценки ситуаций и создана памятка.

Практическая часть показала, что разные цифровые ситуации имеют общую структуру. Во многих случаях пользователя пытаются заставить действовать быстро. Поэтому важнейшей привычкой становится пауза перед действием и независимая проверка информации.

Цель исследовательской работы достигнута: теоретические сведения преобразованы в практический информационный продукт. Гипотеза получила практическое подтверждение на уровне разработанной модели: представление правил через анализ конкретной ситуации помогает связать абстрактное правило с конкретным действием.

Главный вывод: цифровая безопасность начинается с нескольких устойчивых привычек — не спешить, проверять источник, не передавать секретные данные, защищать аккаунты и устройства, контролировать цифровой след и своевременно обращаться за помощью.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Актуальная редакция на 2026 г. // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 24.09.2026).

2. Банк России. Мошенники звонят под видом Центробанка (ЦБ): действия финансовых мошенников. Обновлено 16.07.2026. URL: https://www.cbr.ru/information_security/pmp/ (дата обращения: 24.09.2026).

3. Банк России, ФИНЦЕРТ. Отчёт центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере. Материалы о социальной инженерии и фишинге. URL: https://www.cbr.ru/collection/collection/file/32087/fincert_report_20191010.pdf (дата обращения: 24.09.2026).

4. Минпросвещения России. Меры по просвещению школьников, родителей и учителей в области информационной безопасности. 02.04.2025. URL: https://edu.gov.ru/press/9633/v-moskve-obsudili-mery-po-prosveshcheniyu-shkolnikov-ih-roditeley-i-uchiteley-v-oblasti-informacionnoy-bezopasnosti/ (дата обращения: 24.09.2026).



5. Минпросвещения России. Ирина Шварцман: школьников учат не попадаться на уловки мошенников. 24.12.2025. URL: https://edu.gov.ru/press/10909/irina-shvarcman-shkolnikov-uchat-ne-popadatsya-na-ulovki-moshennikov/ (дата обращения: 24.09.2026).

6. UNICEF. Keeping children safe online. URL: https://www.unicef.org/protection/keeping-children-safe-online (дата обращения: 24.09.2026).

7. UNICEF. Children and online privacy. 2019. URL: https://www.unicef.org/childrightsandbusiness/reports/children-and-online-privacy (дата обращения: 24.09.2026).

8. CISA. Secure Our World: базовые действия для безопасности в сети. URL: https://www.cisa.gov/secure-our-world (дата обращения: 24.09.2026).

9. CISA. Turn On MFA. URL: https://www.cisa.gov/secure-our-world/turn-mfa (дата обращения: 24.09.2026).

10. UNICEF. Cyberbullying: What is it and how to stop it. URL: https://www.unicef.org/stories/how-to-stop-cyberbullying (дата обращения: 24.09.2026).

11. UNICEF Parenting. How to talk to your child about cyberbullying. URL: https://www.unicef.org/parenting/child-care/what-to-do-if-your-child-is-experiencing-cyberbullying (дата обращения: 24.09.2026).

12. CISA. Secure Our World: Passwords Tip Sheet. URL: https://www.cisa.gov/sites/default/files/2024-09/Secure-Our-World-Passwords-Tip-Sheet.pdf (дата обращения: 24.09.2026).

13. Минпросвещения России. Проект «Цифровой ликбез» поможет научить детей правилам безопасного поведения в интернете. 01.06.2022. URL: https://edu.gov.ru/press/5258/proekt-cifrovoy-likbez-pomozhet-nauchit-detey-pravilam-bezopasnogo-povedeniya-v-internete/ (дата обращения: 24.09.2026).

ПРИЛОЖЕНИЕ 1.

**ПАМЯТКА**
**10 ПРАВИЛ ЦИФРОВОЙ БЕЗОПАСНОСТИ ПОДРОСТКА**

| № | Правило | Что сделать |
|---|---|---|
| 1 | Не спеши | Если тебя торопят - остановись и проверь |
| 2 | Береги секретное | Не передавай пароли и коды подтверждения. |
| 3 | Проверяй ссылки | Не переходи по неожиданным ссылкам; открой сервис самостоятельно. |
| 4 | Используй уникальные пароли | Не повторяй один пароль на разных важных аккаунтах. |
| 5 | Включай MFA | Добавь второй способ подтверждения входа. |
| 6 | Обновляй устройства | Устанавливай обновления системы и приложений. |
| 7 | Думай перед публикацией | Проверь фон, геометки и аудиторию. |
| 8 | Добавь второй способ подтверждения входа. | Необычную просьбу знакомого подтверждай другим способом. |
| 9 | Сохраняй доказательства | При травле или мошенничестве сохрани сообщения. |
| 10 | Проси помощи | При угрозе, взломе или мошенничестве обратись к взрослому и в официальный сервис. |

ОСТАНОВИСЬ → ПРОВЕРЬ → НЕ ПЕРЕДАВАЙ СЕКРЕТНОЕ → ОБРАТИСЬ ЗА ПОМОЩЬЮ.

ПРИЛОЖЕНИЕ 2.

## ЧЕК-ЛИСТ САМОПРОВЕРКИ

Отметь выполненные пункты. Если ответ «нет», это не повод для паники: чек-лист нужен, чтобы постепенно улучшать цифровую безопасность.

☐ 1. На устройстве установлена блокировка экрана.

☐ 2. Я не использую один пароль для всех важных аккаунтов.

☐ 3. На важных аккаунтах включена MFA, если она доступна.

☐ 4. Я знаю, как проверить активные сеансы.

☐ 5. Я не передаю пароли и коды подтверждения.

☐ 6. Я умею распознавать сообщение, которое пытается меня торопить или напугать.

☐ 7. Я не ввожу пароль на странице из неожиданной ссылки, пока не проверю адрес.

☐ 8. Необычные просьбы знакомых я подтверждаю другим способом.

☐ 9. Я устанавливаю обновления системы и приложений.

☐ 10. Я проверяю разрешения приложений.

☐ 11. Перед публикацией фотографии я проверяю фон и геометки.

☐ 12. Я понимаю, какая информация в профиле доступна незнакомым людям.

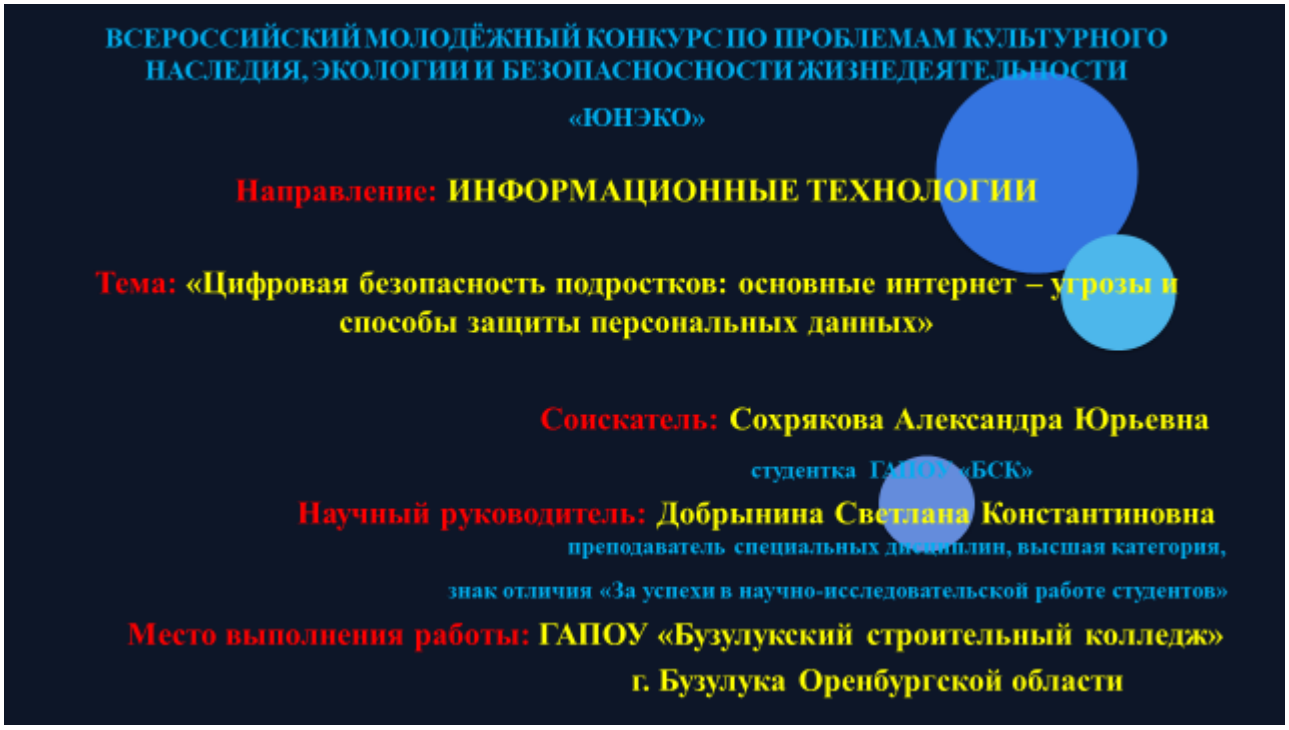
☐ 13. Я знаю, кому из взрослых могу рассказать о проблеме.

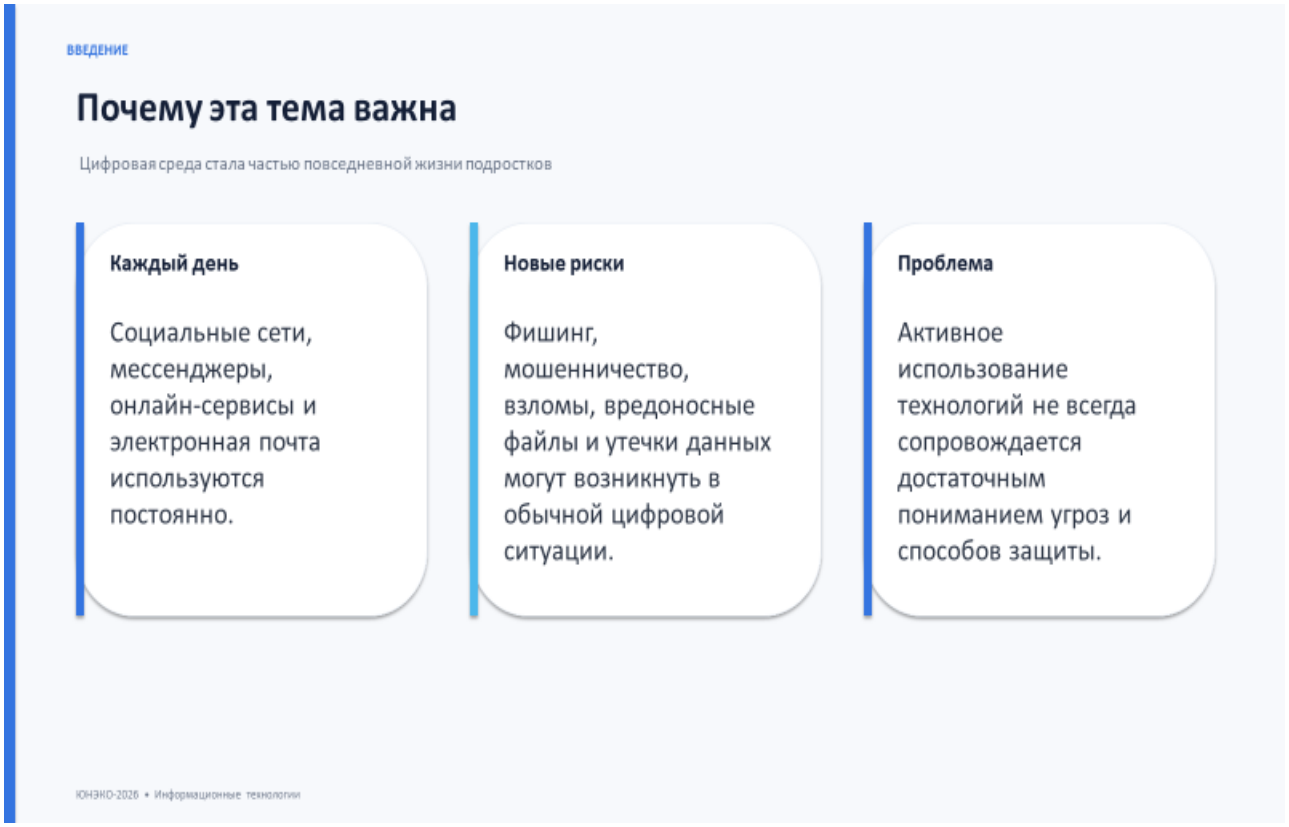
☐ 14. Я знаю, что при травле важно сохранить доказательства.

☐ 15. Я знаю, что при финансовом мошенничестве нужно быстро обратиться в банк через официальный канал.

Итог: _____ из 15. Что я улучшу в первую очередь: _____

ПРИЛОЖЕНИЕ № 3



ИССЛЕДОВАНИЕ

## Цель и задачи

**Цель**

Изучить основные интернет-угрозы, определить доступные способы защиты данных, аккаунтов и устройств и разработать практические рекомендации для подростков.

**Что изучается**

1. Цифровая безопасность
2. Персональные данные и цифровой след
3. Основные интернет-угрозы
4. Способы защиты

**Что создаётся**

5. Анализ типичных ситуаций
6. Памятка «10 правил»
7. Чек-лист самопроверки

ТЕОРИЯ

## Что такое цифровая безопасность?

**Защита**

Цифровая безопасность — это знания, правила и меры, которые помогают защищать персональные данные, аккаунты, устройства и другую информацию.

**Что защищаем**

- аккаунты
- пароли
- устройства
- персональные данные
- цифровой след

**От чего?**

- мошенничества
- фишинга
- взлома
- вредоносных файлов
- утечек данных

УГРОЗЫ

## Основные интернет-угрозы

**Фишинг**

Поддельные ссылки и сайты

**Социальная инженерия**

Манипуляция человеком

**Взлом аккаунта**

Кража доступа

**Мошенничество**

Обман ради денег или данных

**Вредоносные файлы**

Опасные программы

**Фальшивые аккаунты**

Выдача себя за другого

УГРОЗЫ

## Как выглядит опасная ситуация?

**Подозрительное сообщение**

«Ваш аккаунт будет заблокирован! Срочно перейдите по ссылке и подтвердите данные.»

Признаки: давление, срочность, ссылка, запрос данных.

**Безопасная реакция**

Не переходить по ссылке.
Не сообщать пароль или код.
Проверить информацию через официальный сервис.
Не действовать под давлением.

ЗАЩИТА

07

## Защита аккаунтов и устройств

**Надёжные пароли**

Создавать сложные комбинации

**Разные пароли**

Не повторять пароль на разных сервисах

**MFA**

Включать многофакторную аутентификацию

**Коды**

Никому не сообщать коды подтверждения

**Обновления**

Своевременно обновлять ПО

**Сеансы**

Проверять подключённые устройства



ЗАЩИТА

## Персональные данные и цифровой след

**Что может раскрывать слишком много?**

Место учёбы • адрес • номер телефона • документы • фотографии • распорядок дня • поездки • информация о семье

**Что делать?**

Проверять фон фотографий
Ограничивать доступ к профилю
Проверять подписчиков
Удалять ненужную информацию
Контролировать разрешения приложений

**Цифровой след формируется не только публикациями, но и другими действиями в интернете.**

ПРАКТИКА

## Собственная схема анализа цифровых ситуаций

| СИТУАЦИЯ | ПРИЗНАКИ | РИСК | ДЕЙСТВИЕ |
|---|---|---|---|
| Что произошло? | Что вызывает подозрения? | Что может произойти? | Как поступить безопасно? |

**Схема позволяет не просто перечислять правила, а применять их к реальной ситуации.**

ПРАКТИКА

## Анализ типичных цифровых ситуаций

| | | |
|---|---|---|
| **Подозрительная ссылка** | Фишинг | Не переходить; проверить официальный источник |
| **Код из SMS** | Захват аккаунта | Никому не сообщать код |
| **Неожиданный файл** | Вредоносное ПО | Не открывать |
| **Просьба от знакомого** | Взлом аккаунта | Проверить другим способом |
| **Неизвестный вход** | Компрометация | Сменить пароль + завершить сеансы |

В исследовательской работе рассмотрено 10 типичных ситуаций; выше — ключевые примеры.

ПРАКТИКА

## Авторская памятка: 10 правил цифровой безопасности

- ✓ Использовать надёжные пароли
- ✓ Не использовать один пароль везде
- ✓ Включать MFA
- ✓ Никому не сообщать коды
- ✓ Проверять ссылки
- ✓ Не открывать неизвестные файлы
- ✓ Проверять отправителя
- ✓ Не публиковать лишние данные
- ✓ Контролировать приватность
- ✓ При сомнении — остановиться и проверить

ПРАКТИКА

## Чек-лист самопроверки

- □ У меня разные пароли для важных аккаунтов
- □ Включена многофакторная аутентификация
- □ Я не сообщаю коды подтверждения
- □ Я проверяю ссылки перед переходом
- □ Устройства и приложения обновляются
- □ Настройки приватности проверены
- □ Я умею завершать неизвестные сеансы
- □ Я знаю, что делать при взломе

Чек-лист помогает самостоятельно оценить базовый уровень цифровой безопасности.

РЕЗУЛЬТАТЫ

## Что получилось в результате исследования?

### Систематизация

Выделены основные группы интернет-угроз и признаки опасных цифровых ситуаций.

### Собственный подход

Разработана схема : «ситуация → признаки → риск → безопасное действие

### Практический продукт

Созданы памятка «10 правил» и чек-лист самопроверки.

ВЫВОД

## Основной вывод

**Цифровая безопасность зависит не только от технических средств защиты, но и от поведения самого пользователя.**

Знание признаков угроз, внимательное отношение к персональным данным и соблюдение базовых правил помогают снизить риск распространённых цифровых проблем.

### Практично

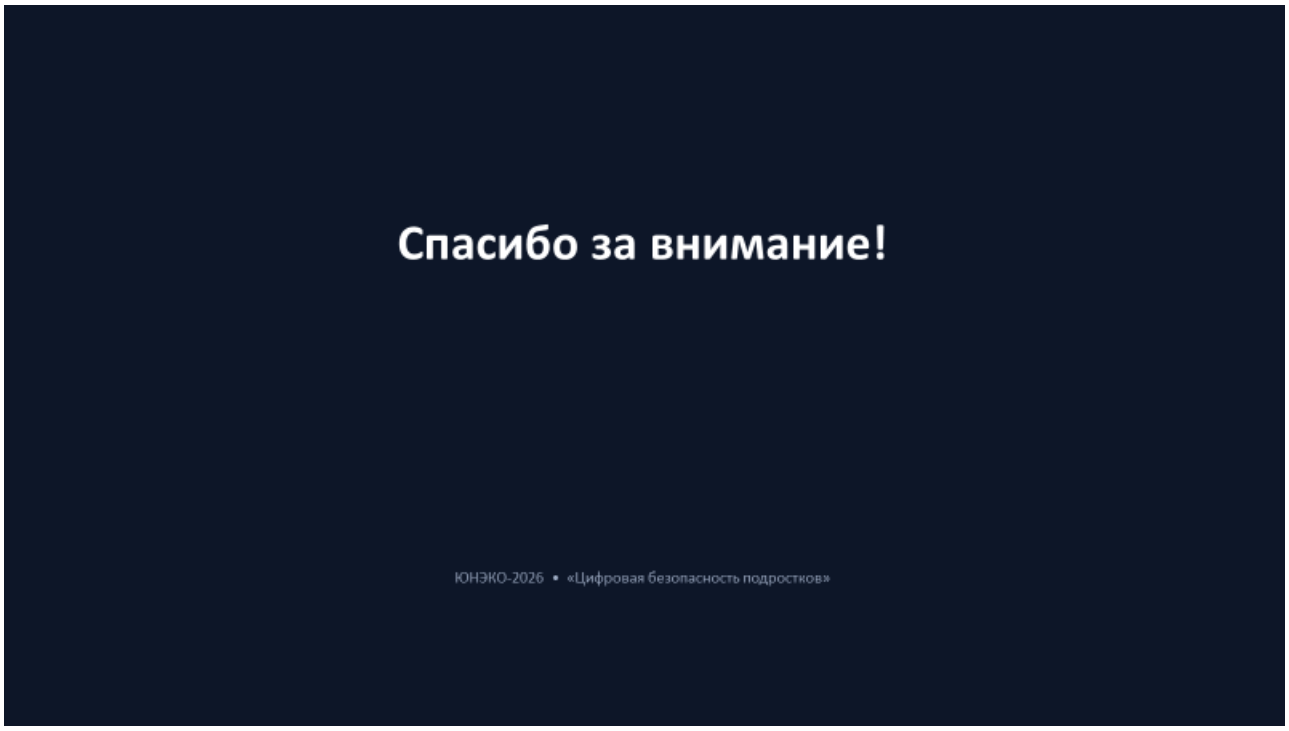
Памятка + чек-лист

### Понятно

Алгоритм действий

### Применимо

Повседневная цифровая среда


Спасибо за внимание!
ЮНЭКО-2026 • «Цифровая безопасность подростков»