

# Методика обучения школьников основам безопасности в сети Интернет

**Целью исследования** является обоснование и апробирование интерактивной методики, предполагающей активное взаимодействие старшеклассника – модератора и школьников в процессе формирования у них компетенций в области информационной безопасности, позволяющих им успешно социализироваться в информационной среде. Актуальность данной проблемы обусловлена, с одной стороны, процессом информатизации всех сфер жизнедеятельности общества и востребованностью в этой связи субъектов общества, обладающих как знаниями в сфере информационной безопасности, так и способностью обеспечивать собственную технологическую, идеологическую и психологическую безопасность и на этой основе объективно анализировать и оценивать поступающую к ним информацию с учетом содержащихся в ней угроз. С другой – потребностью практики в методическом обеспечении процесса обучения школьников основам безопасности в сети Интернет и недостаточной разработанностью данного вопроса в педагогической науке.

**Материалы и методы.** Для достижения поставленной цели мы использовали системный подход для построения модели интерактивной методики обучения школьников основам информационной безопасности, деятельностный подход, позволяющий активизировать процесс взаимодействия субъектов познавательной деятельности и возможность повышения его эффективности на основе геймификации. В работе применялись следующие методы: анализ педагогической, психологической, научно-технической и методической литературы по проблеме исследования, систематизация, обобщение, эксперимент, анкетирование, тестирование, опрос, диагностические методики (методики интернет-зависимости С.А. Куликова и Кимберли-Янг в адаптации С.А. Лоскутовой), методы математической статистики и наглядного представления результатов. В эксперименте были задействованы 66 школьников с пятого по девятый классы и

5 старшеклассников в качестве модераторов школы № 28 г. Магнитогорска.

**Результаты.** В рамках исследования разработана и апробирована интерактивная методика обучения школьников основам безопасности в сети Интернет, реализуемая в рамках внеурочной деятельности на основе авторской программы, разработанной на спиралевидном принципе представления содержания обучения, взаимодействия учителя, старшеклассника – модератора и школьников на принципе наставничества, с использованием геймификации. Разработанный нами гейм-сценарий на принципах постепенного усложнения ситуационных заданий в зависимости от возраста школьников (механика геймификации), сотрудничества (динамика геймификации) и мотивации (компоненты геймификации), реализован в виде мобильного приложения с элементами дополнительной реальности. В рамках данной методики ученики старшего звена выступают наставниками для обучающихся среднего школьного возраста. Изучение мнения школьников свидетельствует о том, что они удовлетворены процессом и результатом обучения.

**Заключение.** Предлагаемая интерактивная методика обучения школьников основам безопасности в сети Интернет, сочетающая элементы традиционного и электронного обучения в рамках внеурочной деятельности, обеспечивает вовлечение школьников в учебный процесс на основе развития внешней и внутренней мотивации, повышает продуктивность их познавательной деятельности, исключает формализм в интерактивном взаимодействии и позволяет эффективно реализовать контроль и оценку результатов обучения.

**Ключевые слова:** информационная безопасность, компетенция, электронное обучение, модель интерактивной методики обучения, концентрический принцип, спиралевидный принцип, ситуационные задания, геймификация.

Marina V. Romanova, Elena V. Chernova

Magnitogorsk State Technical University named after G.I. Nosov, Magnitogorsk, Russia

## The Method of Teaching Schoolchildren the Basics of Security on The Internet

**The purpose of the study** is to substantiate and test an interactive methodology that involves the active interaction of a high school student – a moderator and schoolchildren in the process of developing their competencies in the field of information security, allowing them to successfully socialize in the information environment. The relevance of this problem is due, on the one hand, to the process of informatization of all spheres of society's life and the demand in this regard for the subjects of society who have both knowledge in the field of information security and the ability to ensure their own technological, ideological and psychological security and, on this basis, objectively analyze and evaluate information coming to them, taking into account the threats contained in it. On the other hand, the need for practice in the methodological support of the process of teaching schoolchildren the basics of security on the Internet and the insufficient development of this issue in pedagogical science.

**Materials and methods.** To achieve this goal, we used a systematic approach to create a model of an interactive methodology for teaching schoolchildren the basics of information security, an activity approach that allows us to activate the process of interaction between subjects

of cognitive activity and the possibility of increasing its effectiveness based on gamification. The following methods were used in the work: analysis of pedagogical, psychological, scientific, technical and methodological literature on the research problem, systematization, generalization, experiment, questioning, testing, survey, diagnostic methods (methods of Internet addiction by S. Kulikov and Kimberly-Young in adapted by S. Loskutova), and methods of mathematical statistics and visual presentation of results. The experiment involved 66 schoolchildren from the fifth to the ninth grades and five high school students as moderators of school No. 28 in Magnitogorsk.

**Results.** As part of the study, an interactive methodology for teaching schoolchildren the basics of Internet security was developed and tested, implemented as part of extracurricular activities based on the author's program, developed on the spiral principle of presenting the content of training, interaction between a teacher, a high school student – moderator and schoolchildren on the principle of mentoring, using gamification. The game scenario developed by us on the principles of gradual complication of situational tasks depending on the age of schoolchildren (gamification mechanics), cooperation

(gamification dynamics) and motivation (gamification components) is implemented as a mobile application with elements of additional reality. Within the framework of this methodology, senior students act as mentors for students of middle school age. The study of the opinions of schoolchildren indicates that they are satisfied with the process and the result of education.

**Conclusion.** The proposed interactive methodology for teaching schoolchildren the basics of security on the Internet, combining elements of traditional and e-learning as part of extracurricular activities, ensures

the involvement of schoolchildren in the educational process based on the development of external and internal motivation, increases the productivity of their cognitive activity, eliminates formalism in interactive interaction and allows effective implement monitoring and evaluation of learning outcomes.

**Keywords:** information security, competence, e-learning, model of interactive teaching methodology, concentric principle, spiral principle, situational tasks, gamification.

## Введение

Россия, как и многие страны, идет в своем развитии к цифровому обществу, которое характеризуется, в первую очередь, высокой скоростью коммуникационных процессов, обеспечивающийся информационными технологиями и сетью Интернет. Интернет, являясь средством многократного увеличения возможности и скорости осуществления коммуникаций, решает одну из важнейших проблем цифрового общества — генерации, обработки и передачи огромного массива информации, которая становится главным ресурсом в современном обществе.

Анализируя материалы электронного ресурса «Вся статистика интернета и соцсетей на 2021 год — цифры и тренды в мире и в России» приходим к выводу, что сегодня в мире насчитывается 4,20 млрд пользователей социальных сетей, а это около 53,6% всего населения мира. Для человека, особенно в условиях пандемии, Интернет создал уникальные возможности для саморазвития, образования, самообразования и трудовой деятельности, информационного обмена, социальной коммуникации и сотрудничества.

Данная сеть наполнена не только полезной информацией, она одновременно выступает каналом трансляции угроз и рисков, которые практически беспрепятственно существуют в Интернете и активно воздействуют на различные категории пользователей. Это порождает проблему информационной безопасности, ко-

торая охватывает все области общественной жизни, поэтому компетенции в сфере защиты информации требуются не только от IT-специалистов, но и от любого пользователя персональным компьютером, что отражено в стратегии развития информационного общества РФ на период с 2017 до 2030 года.

В силу возраста наиболее уязвимой категорией в области информационной безопасности выступают подростки, для которых сеть Интернет стала естественной коммуникационной средой, оказывающей влияние на их мировоззрение и поведение. Сегодня 56% школьников в мире имеют собственные аккаунты в социальной сети, за последние три года, как отмечает Росстат, количество домашних хозяйств в России с доступом в интернет за последние 3 года выросло в среднем на 4%, из них с помощью мобильного устройства на 15%. Средний возраст школьников, которые входят в учетную запись, составляет 12,6 года. Но при всем этом уровень их компетенции в сфере информационной безопасности недостаточный для того, чтобы безопасно использовать привычные и наиболее популярные информационные ресурсы. Так опасности, с которыми сталкиваются школьники в сети со стороны СМИ, сектантов, «сообществ смерти», активно провоцирующих суицидальные действия, тематических групп, стимулирующих различного рода аддикции, а также вредоносный контент, могут оказать неисправимое на них воздей-

ствие. Например, количество сексуальным домогательствам, совершенных против несовершеннолетних с 2014 года выросло на 44%, жертвами интернет-мошенников стали 54% опрошенных детей в возрасте до 18 лет.

Следовательно, наибольшей опасностью развития цифровых технологий является разрастающаяся проблема обеспечения информационной безопасности на всех уровнях — от личной до государственной. Комплекс законодательных и организационно-правовых мер в данной сфере направлен на снижение риска негативного влияния, которое может получить ребенок в сети Интернет [1].

Анализ научной литературы позволяет констатировать, что проблема информационной безопасности является междисциплинарной. Так, общим вопросам информационной безопасности посвящены исследования Э. Брандмана, Г.Г. Гафарова, Д.П. Зегжда, В.П. Петрова, С.В. Петрова, С.П. Расторгуева, В.В. Смелянской и др. В данных работах раскрыты информационные угрозы, факторы их вызывающие, а информационная угроза рассматривается как состояние защищенности жизненно важных интересов государства, общества и личности в информационной сфере от влияния внешних и внутренних факторов [2, 3, 4, 5, 6 и др.].

Изучению информационной безопасности личности посвящены исследования многих ученых. Причем, если еще лет пять назад основное внимание ученых было направ-

ленно на обсуждение вопросов подготовки студентов и старшеклассников к безопасному использованию сети Интернет, то сегодня информационная безопасность подростков становится приоритетной задачей не только государства, но и педагогической науки.

Ведущая роль в обучении школьников основам информационной безопасности в сети Интернет принадлежит школе, имеющей для этого значительные возможности. Соответственно, возникает проблема эффективного обучения подростков основам информационной безопасности как в рамках уроков информатики, так и внеурочной работы.

Анализ научно-педагогической и психологической литературы показал, что ученые, рассматривая процесс формирования информационной безопасности школьников, акцентируют внимание, либо на особенностях социализации современных подростков в условиях стремительно нарастающих информационных потоков, их психического состояния, прежде всего в информационном пространстве, либо рассматривают отдельные содержательно-методические аспекты в образовательном процессе.

Так, Е.Г. Белякова, Э.В. Загвязинская и А.И. Березенцева, изучая состояния информационной безопасности школьников, выявили роль внешних ограничений и возможностей внутриличностной фильтрации вредоносного интернет-контента в зависимости от возраста детей [7].

Использованию интерактивных методов при обучении школьников основам информационной безопасности посвящены исследования Х.Н. Арова, Т.Ю. Деншиковой, М.В. Должиковой, И.А. Глущенко, В.А. Петькова, А.С. Доколин, А.Н. Старков [8, 9].

В.Ю. Кузнецова акцентирует внимание на обучение

школьников криптографическим методам защиты информации (шифры перестановки, подстановки, аналитические преобразования и гаммирование) с использованием учебно-демонстрационного программного продукта [10].

О.С. Петрова рассматривает возможности этических подходов (утилитарного и деонтологического) для обеспечения информационной безопасности школьников в условиях обучения с применением дистанционных образовательных технологий и с учетом специфики реализуемых образовательных программ [11].

Заслуживает внимания опыт организации учебного процесса на основе использования геймификации, являющейся вариантом смешанного обучения, предполагающего сочетание элементов традиционного и электронного обучения [12, 13, 14 и др.].

Контент-анализ приведенных работ, а также исследования других ученых позволяет говорить о том, что в теоретических исследованиях имеется ряд интересных наработок, однако проблема эффективности обучения школьников основам информационной безопасности в сети Интернет остается недостаточно разработанной. Следовательно, мы можем констатировать противоречие, обусловленное, с одной стороны, процессом информатизации всех сфер жизнедеятельности общества и востребованностью в этой связи субъектов общества, обладающих как знаниями в сфере информационной безопасности, так и способностью обеспечивать собственную технологическую, идеологическую и психологическую безопасность и на этой основе объективно анализировать и оценивать поступающую к ним информацию с учетом содержащихся в ней угроз. С другой — потребностью практики в методическом обеспечении процесса обучения школьни-

ков основам безопасности в сети Интернет и недостаточной разработанностью данного вопроса в педагогической науке.

Данное противоречие определило проблему исследования, которая заключается в поиске и научном обосновании принципов, содержания и технологии обучения школьников основам безопасности в сети Интернет в рамках внеурочной деятельности.

## Основная часть

Целью исследования является обоснование и апробирование интерактивной методики, предполагающей активное взаимодействие старшеклассника — модератора и школьников в процессе формирования у них компетенций в области информационной безопасности, позволяющих им успешно социализироваться в информационной среде.

Разработка интерактивной методики осуществлялась с позиции системного подхода [15, 16 и др.], который позволяет рассмотреть процесс обучения школьников основам безопасности в сети Интернет как целостную систему, понять цель ее существования, функции, свойства, структуру и спроектировать ее модель. При проектировании модели методики обучения школьников основам безопасности в сети интернет мы учитывали, что научная модель представляет собой абстрагированное выражение сущности исследуемого явления. В исследовании степень подобия модели реальной действительности была соотнесена с целью исследования и определен тип проектируемой модели — модель структурно-содержательного типа. Спроектированную нами модель мы рассматриваем как подсистему открытого типа, встроенную в контекст образовательной системы школы, реализующуюся в рамках внеурочной деятельности. Мо-



дель представлена четырьмя взаимосвязанными блоками: блок исходных оснований, субъектный блок, содержательно-технологическим и результативным.

В блок *исходных оснований* мы включили целевой и теоретический компоненты.

Определяя цели и задачи, мы учитывали, что компетенция — это знания в действии, способность человека использовать их на практике, применять умения и навыки для решения различных задач [17, 18 и др.]. Под информационной безопасностью понимают «состояние и условия жизнедеятельности личности, при которых реализуются ее информационные права на свободный доступ и размещение информации; обеспечивается состояние защищенности конфиденциальной информации, которой владеет личность; отсутствует угроза причинения личности вреда информацией» [19 с. 239]. Выделяют три составляющие информационной безопасности личности: информационно-техническая, информационно-идеологическая и информационно-психологическая [20].

*Цель* — формирование у школьников компетенций в области информационной безопасности.

*Задачи:*

- обобщить и сформировать знания, умения и навыки безопасного нахождения в сети интернет;
- обучить школьников правилам безопасного нахождения в сети;
- сформировать представление о возможных угрозах в сети;
- научить школьников распознавать возможные угрозы в сети Интернет и правильно реагировать на них;
- закрепить полученные ранее знания на практике;
- сформировать представление о цифровом пространстве и возможных угрозах в нем;

- научить школьников безопасно искать информацию, взаимодействовать с другими пользователями в сети;

- подготовить школьников к безопасному использованию Интернета.

В результате обучения школьник должен:

- знать основные правила безопасного поведения в сети Интернет;
- знать, уметь распознавать, предотвращать возможные угрозы в сети;
- правильно реагировать на возникающие опасности в сети Интернет;
- уметь безопасно работать в сети с информацией, другими пользователями, программами;
- соблюдать правила безопасного нахождения в сети;
- сознательно и бережно относиться к вопросам собственной информационной безопасности;
- соблюдать моральные нормы и правила поведения в Интернете.

*Формируемые универсальные учебные действия*

*Личностные:*

- формирование ответственного отношения к учению;
- способность связать изученное с собственным жизненным опытом;
- владение первичными навыками анализа;
- формирование готовности и способности к саморазвитию и самообразованию на основе мотивации к обучению и познанию;
- проявление дисциплинированности и трудолюбия;
- формирование заинтересованности в достижении успеха и победы;
- формирование лидерских качеств.

*Познавательные:*

- изучение правил безопасного нахождения в сети;
- изучение возможных угроз, с которыми можно столкнуться в сети;

- умение правильно реагировать на возникающие опасности в сети;

- изучение мер и способов предотвращения возникновения угроз;

- формирование умения ориентироваться в Интернет-пространстве.

*Коммуникативные:*

- развитие коммуникативных навыков при работе в группе,
- умение слушать друг друга;
- активное включение в общение и взаимодействие со сверстниками на принципах уважения и доброжелательности, взаимопомощи и сопереживания.

Теоретический компонент представлен нами системным и деятельностным подходами, а также базовыми принципами, на которые мы опирались при организации процесса обучения школьников информационной безопасности: принцип спиралевидного представления содержания обучения, постепенного усложнения заданий, наставничества, сотрудничества и мотивации.

*Субъектный блок* определяет коммуникативный аспект предлагаемой нами интерактивной методики обучения школьников основам безопасности в сети Интернет, как взаимодействие учителя, старшеклассника — модератора и школьников.

Учитель, как наставник старшеклассников, помогает им в организационном плане, объясняя принцип проведения очных этапов геймификации, выдает перечень заданий для каждого этапа и методику оценивания результатов.

Старшеклассники, выступая модераторами игроков средних классов, объясняют, помогают, координируют школьников в процессе прохождения гейм-сценария и оценивают выполнение заданий.

В *содержательно-технологический блок* мы включили содержание авторской про-

**Анализ теоретической базы**  
**Analysis of the theoretical base**

| Класс   | Изучаемые разделы                                                                                                                                                                                                                                                                                                                      | Актуальность внедрения методики                                                                                                                                                                                                                                                                                                         |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5 класс | Разделы: теоретической информатики (формы представления и действия с информацией), средства информатизации (устройство компьютера) и информационные технологии. Планируемые результаты по окончании прохождения курса: формирование навыков безопасного и целесообразного поведения при работе с компьютерными программами в Интернете | Внеурочная деятельность будет актуальна в качестве закрепления полученных знаний безопасного нахождения в сети                                                                                                                                                                                                                          |
| 6 класс | Разделы: информация вокруг нас, информационные технологии, информационное моделирование, алгоритмизация                                                                                                                                                                                                                                | Полученные навыки в 5 классе по безопасному нахождению в сети можно актуализировать в рамках темы информационные технологии во внеурочной деятельности. Закрепив уже изученный материал, необходимо дополнить новыми правилами, которые будут уже актуальны для 6 класса                                                                |
| 7 класс | В начале года школьники изучают информационные процессы, затем мультимедию, основы программирования и алгоритмизации. В рамках темы «Информация и информационные процессы» есть урок посвященные всемирной паутине                                                                                                                     | На данном этапе прохождения дисциплины школьники изучают поиск информации в Интернете, поэтому для них будет актуальным повторение изученных ранее в 6 классе правил безопасного использования сети Интернет и изучение новых                                                                                                           |
| 8 класс | Изучение алгоритмизации, программирования и логических операций                                                                                                                                                                                                                                                                        | На этом этапе изучения информатики школьники разовьют навыки построения логических цепочек, поэтому для них будет актуально рассмотрение причинно-следственных связей в области безопасного нахождения в сети, которые затрагивают сложные схемы обмана кибер-преступниками, их психологическое воздействие для достижения своей выгоды |
| 9 класс | Изучаемые темы: моделирование, обработку числовой информации и коммуникационные технологии                                                                                                                                                                                                                                             | В рамках раздела коммуникационные технологии особенно актуально будет изучение правил безопасного нахождения в сети, а также закрепление рассмотренных тем в рамках учебной программы: сетевой этикет, электронная почта, сетевое коллективное взаимодействие                                                                           |

граммы, реализующейся во внеурочной деятельности, комплекс усложняющихся ситуационных заданий (содержательный компонент) и геймификацию (технологический компонент).

Рассмотрим учебно-методические планы по информатике различных классов (табл. 1), чтобы актуализировать проведение внеурочной деятельности по основам безопасного нахождения в сети Интернет.

Анализируя содержание учебников на предмет отражения в них требований стандартов в области обучения вопросам информационной безопасности школьников в рамках предмета информатика, мы пришли к выводу, что авторы учебников по информатике предпочитают использовать концентрический принцип в преподавании разделов, относящихся к данной проблематике, часто повторяя содержание по данному разделу в неизменном виде на всех этапах основной школы.

Полагаем, что предпочтительнее использовать спиралевидный принцип обучения для обеспечения соответствия уровня сложности материала возрастным особенностям школьников с углублением содержания раскрываемых понятий во внеурочной деятельности. Такое представление содержания поддержит интерес школьников, будет способствовать расширению их кругозора, актуализирует мотивацию к восприятию нового материала, развивает их творческие способности. Разработанное нами содержание авторской программы по основам безопасности в сети Интернет, с учетом данных табл. 1, представлено следующими модулями: безопасность личности в цифровом пространстве; законодательные аспекты кибербезопасности; защита информации (табл. 2).

Содержание программы подкреплено ситуационными

заданиями с учетом возрастных особенностей школьников, уровня полученных знаний в области информационной безопасности. Ситуационные задания отражают практическую ситуацию, которая направлена на получение нового знания о ситуации в сфере информационной безопасности и понимания поведения в ней. При составлении ситуационных заданий мы учитывали, что они могут быть сюжетными,

причем одну сюжетную линию может иметь набор задач, решение которых предполагается на протяжении темы или даже целого модуля [21, 22].

Технологический компонент данного блока представлен геймификацией. Геймификация — это технология обучения, которая рассматривается учеными как метод обучения, форма воспитания, и как средство организации целостного образовательно-

Таблица 2 (Table 2)

**Содержание учебной программы**  
**Content of the curriculum**

| Наименование учебных модулей                     | Наименование тем модуля                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Безопасность личности в цифровом пространстве | 1.1. Информационное общество<br>1.2. Основы информационного поиска<br>1.3. Сайты-клоны, надежные ресурсы: отличия и отбор<br>1.4. Информационная безопасность и кибербезопасность<br>1.5. Информационное манипулирование<br>1.6. Способы воздействия и защиты личности<br>1.7. Информационно-психологическая безопасность<br>1.8. Защита физического здоровья в классе и дома |
| 2. Законодательные аспекты кибербезопасности     | 2.1. Основы информационного права<br>2.2. Авторское право<br>2.3. Киберпиратство<br>2.4. Антиплагиат                                                                                                                                                                                                                                                                          |
| 3. Защита информации                             | 3.1. Информационные угрозы<br>3.2. Безопасная работа с браузером<br>3.3. Разграничение доступа<br>3.4. Безопасная работа на чужом устройстве<br>3.5. Вредоносные программы и защита от них<br>3.6. Хранение данных<br>3.7. Носители информации<br>3.8. Платежные системы в Интернет                                                                                           |

го процесса, реализующееся через игровые элементы и в условиях игрового дизайна. Учеными подчеркивается, что геймификация — это не игра, а общая игровая оболочка целенаправленного процесса [23]. Выделяют два вида геймификации в образовании:

— полное погружение, когда весь урок проходит в игровой форме;

— легкое погружение, когда по ходу урока игровые методики применяются частично, то есть совместно с классическими методами обучения.

В предлагаемой нами методике используется второй вариант, поскольку он позволяет сочетать положительные стороны традиционного и электронного обучения в рамках внеурочной деятельности [24, 25]. Внедряя геймификацию в учебный процесс, мы учитывали, что в основе данной педагогической технологии лежат три важных элемента: динамика, механика и компоненты [13].

Механика, определяя «правила» игры и отражая порционность подачи учебного материала с опорой на принцип постепенного усложнения си-

туационных заданий, задает ограниченное время выполнения отдельного этапа. Динамика описывает ход игры, когда правила начали действовать, особенности взаимодействия участников (принцип сотрудничества), получение достижений. Компоненты — это очки, баллы, статусы, награды и т.д. (принцип мотивации).

Мы разработали собственный сценарий игры «Safety First» с дополненной реальностью, которая сможет сформировать знания школьников, развить у них умения и навыки в сфере информационной безопасности, привлечь их внимание к теме безопасного Интернета и мотивировать на изучение нового материала. Данный сценарий подойдет для реализации только в мобильном приложении, потому что используется технология дополненной реальности при наведении камеры на различные карточки. А очные этапы учебного урока помогают эффективно провести проверку знаний по теме безопасного поведения в сети Интернет с помощью интересных для школьников ситуационных заданий и с опорой на ин-

рактивные методы (дискуссия, круглый стол). Модель проведения игры включает участие учителя как наставника старшеклассников, учащихся 10–11 классов в качестве модераторов и школьников 5–9 классов в роли игроков.

Отметим, что учитель выступает главными наблюдателями за процессом игры, направляет модераторов, корректирует их действия, помогает в проведении и разрешении возникающих трудностей. Учитель также перед началом объясняет ключевые моменты игры «Safety First». Участие школьников 10–11 классов в роли модераторов игры погружает их в тематику Интернет-безопасности, позволяет вспомнить прошедший материал, развивает навыки управления и регулирования действий других школьников, стрессоустойчивость, грамотность устной речи и внимательность.

В контексте игры школьники в роли игроков делятся на несколько команд, выступая в игре за одного персонажа. Игра предполагает участие от одной до четырех команд, которые выступают от одного лица выбранного героя. Цель игроков — совместно победить злодея. Продолжительность игры три дня. Игра проводится в несколько этапов, которые распределены на несколько дней. Благодаря разделению игры на несколько дней школьники погружаются на долгий промежуток времени в мир безопасного Интернета и их внимание будет акцентировано на изучаемой теме не однократно.

Во время игры форма организации деятельности школьников — групповая работа, метод организации деятельности — игровой. Воспитательные результаты — формирование позитивного отношения к базовым ценностям общества, ценностного отношения к своему и чужому личному пространству, уважительное



отношение к окружающим посредством взаимодействия с другими школьниками между собой на уровне класса и старшеклассниками в качестве модераторов.

Оборудование: мультимедиа, проектор, мобильное устройство со скаченным приложением игры «Safety First», раздаточный материал: листы бумаги на каждую команду, ручки, цветные карандаши, фломастеры. Цель игры – закрепить по определенной теме знания школьников об основах безопасности в сети Интернет.

В табл. 3 представлено календарно-тематическое планирование мероприятий в рамках интерактивной методики.

На рис. 1 представлен начальный экран при входе в приложение игры.

Приложение «Safety First» позволит визуализировать

процесс получения баллов и процесс победы над игровым персонажем. Основными критериями успеха будут являться показатель вовлеченности учеников в образовательный процесс и хорошие результаты прохождения викторины. Сама игра представляет собой уровень, на котором расположены 3D модели главного героя и главного злодея. Пользователю доступна информация об очках здоровья главного злодея и кнопка «Сканировать», которая запускает камеру телефона.

Целью игроков является победа над главным злодеем, путем ответов на вопросы ведущего викторины. В зависимости от набранных баллов игроки будут получать специальные карточки. Сканирование определенной карточки отнимает определенное значение здоровья у главного злодея



Рис. 1. Начальный экран игры «Safety First»

Fig. 1. The initial screen of the game "Safety First"

Таблица 3 (Table 3)

Календарно-тематическое планирование  
Calendar-thematic planning

| День   | Содержание деятельности модератора                                                                                                                                                                                                                                                                                                                                    | Содержание деятельности школьника                                                                                                                                                                                                                                                                                                             | Этапы                                         | Результат                                                                                                                                                                                    | Время  |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| 1 день | Модераторы приветствуют школьников, делят на команды класс, проводят первый этап и оценивают результат работы команд, в соответствии с полученными баллами командой выдают карточку с картинкой, проводят второй этап и его оценку, завершают первый день игры                                                                                                        | Школьники делятся на команды, выбирают капитана, придумывают название и логотип, устанавливают приложение «Safety First», проходят первый и второй очные этапы игры, после которых наводят камеру телефона на полученную картинку, после чего на экране происходит бой между злодеем и героем                                                 | Рисование плаката, «Крокодил»                 | Хорошее настроение, развитие восприятия, внимания, познавательного интереса, образного мышления, креативности, работы в команде                                                              | 45 мин |
| 2 день | Модераторы приветствуют школьников, проводят третий этап и оценивают результат работы команд, в соответствии с полученными баллами командой выдают карточку с картинкой, проводят четвертый этап и его оценку, завершают второй день игры                                                                                                                             | Школьники открывают приложение «Safety First», проходят третий и четвертый очные этапы игры, после которых наводят камеру телефона на полученную картинку, после чего на экране происходит бой между злодеем и героем                                                                                                                         | «Безопасный Синквейн», фото-конкурс «Вспышка» | Формирование элементов конструктивного мышления и творческого воображения, развитие коммуникативности, работы в команде, ловкости, быстроты действия, активности                             | 45 мин |
| 3 день | Модераторы приветствуют школьников, проводят пятый этап и оценивают результат работы команд, в соответствии с полученными баллами командой выдают карточку с картинкой, помогают игрокам зайти на «Бой с боссом», если нужно добрать недостающие баллы для победы, завершают игру беседой по теме «Безопасность в сети Интернет» и получают обратную связь от игроков | Школьники открывают приложение «Safety First», проходят пятый очный этап игры, после которого наводят камеру телефона на полученную картинку, после чего на экране происходит бой между злодеем и героем, если у них не хватает баллов для победы, тогда проходят «Бой с боссом», по итогу которого будет определено победила команда или нет | «Safety кроссворд», «Бой с боссом»            | Формирование способности концентрировать, распределять, удерживать и переключать внимание, развитие логического мышления, смекалки, памяти, навыков произвольного и осмысленного запоминания | 45 мин |



Рис. 2. Получение баллов в игре «Safety First»

Fig. 2. Getting points in the game "Safety First"

(рис. 2). Ответив правильно на большинство вопросов, команда сможет победить.

*Результативный блок* интерактивной методики обучения школьников основам безопасности в сети Интернет включает в себя анкеты, тестовые задания, опрос, диагностические методики (методики интернет-зависимости С.А. Куликова и Кимберли-Янг в адаптации С.А. Лоскутовой), методы математической статистики.

## Результаты

В рамках проведенного исследования разработана и апробирована интерактивная методика обучения школьников основам безопасности в сети Интернет во внеурочной деятельности. В процессе эксперимента нами обнаружены факты, свидетельствующие о недостаточном уровне компетенции школьников в сфере информационной безопасности. Об этом свидетельствовало, в частности, то, что больше половины опрошенных школьников (74%) не догадывались о таком мощном окружении информационных опасностей, воздействующих на их сознание и психику. Из числа тех, которые знакомы с проблемой, лишь 11% смогли четко определить, где и когда возможно быть подвергнутым агрессивному информационному воздействию.

Педагогический экспери-

мент по проверке интерактивной методики обучения школьников основам безопасности в сети Интернет во внеурочной деятельности проводился пять лет. В начале эксперимента для проверки компетенций школьников в области информационной безопасности проводился нулевой срез, который показал примерно одинаковый уровень компетенций у школьников контрольной и экспериментальной групп. Для обучения в экспериментальной группе, кроме изучения базового курса информатики, реализовывалась авторская методика во внеурочной деятельности. В контрольной группе обучение осуществлялось только в рамках изучения базового курса информатики. В конце эксперимента был проведен итоговый срез, который показал, что в результате применения разработанной нами интерактивной методики, школьники экспериментальной группы обнаруживают более высокий уровень компетенций, чем школьники кон-

трольной группы (табл. 4).

Проверку гипотезы о том, что применение авторской интерактивной методики обучения школьников основам безопасности в сети Интернет позволяет повысить уровень их компетенций в данной области, мы проверяли с помощью статистического критерия «хи – квадрат». При сравнении частот экспериментальной и контрольной групп табличное (критическое) значение критерия 5,99 при 5 %-м уровне значимости оказалось существенно меньше расчетного 7,12, что свидетельствует о достоверности выдвинутой гипотезы. Изучение мнения школьников свидетельствует о том, что они удовлетворены процессом и результатом обучения.

## Заключение

В ходе исследования было установлено, что проблема обучения школьников основам безопасности в сети Интернет является одной из актуальных проблем в педагогической теории и практике, требующей своего дальнейшего осмысления. Ее актуальность обусловлена, прежде всего, рядом теоретико-методических предпосылок и конкретно-практическими задачами. Подтверждено необходимость и возможность решения данной проблемы в рамках внеучебной деятельности школьников.

Использование геймификации в рамках разработанной нами методики позволяет организовать оптимальное взаимо-

Таблица 4 (Table 4)

Итоговый срез уровня компетенций школьников в сфере информационной безопасности  
the final cut of the level of competence of schoolchildren in the field of information security

| Уровни  | Экспериментальная группа |        | Контрольная группа |        |
|---------|--------------------------|--------|--------------------|--------|
| Низкий  | 5                        | 16,1 % | 10                 | 28 %   |
| Средний | 8                        | 25,8 % | 16                 | 45,7 % |
| Высокий | 18                       | 58,1 % | 9                  | 25,7 % |
|         | 31                       |        | 35                 |        |



действие между школьниками, старшеклассниками — модераторами и учителем. Применение игровых методов для неигровой деятельности способствует вовлечению школьников в процесс обучения, развитию внешней и внутренней мотивации, повышает уровень удовлетворенности процессом, а использование рейтингов способствует стремлению школьников повысить свою позицию за счет выполнения ситуационных заданий, участия в дискуссиях.

Исследование показало, что реализация разработанной нами интерактивной методики

обучения школьников основам безопасности в сети Интернет отличается следующими особенностями: возможностью приблизить процесс обучения к реальной действительности (на основе ситуационных заданий и гейм-сценарий); интенсификацией группового способа обучения; возможностью усиления эмоциональной составляющей обучения; существенной активизацией взаимодействия всех субъектов учебного процесса, неформальностью этого взаимодействия; развитием творческих способностей как ведущих качеств личности.

В целом, предлагаемая нами интерактивная методика обучения школьников основам безопасности в сети Интернет, сочетающая элементы традиционного и электронного обучения в рамках внеурочной деятельности, обеспечивает вовлечение школьников в учебный процесс на основе развития внешней и внутренней мотивации, повышает продуктивность их познавательной деятельности, исключает формализм в интерактивном взаимодействии и позволяет эффективно реализовать контроль и оценку результатов обучения.

## Литература

1. Рыбакова О.С. Законодательное регулирование обеспечения безопасности ребенка в интернет-пространстве // Правовая информатика. 2017. № 4. С. 49–54.
2. Петров В.П., Петров С.В. Информационная безопасность человека и общества: учебное пособие. М.: ЭНАС, 2007.
3. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. М.: Горячая линия-Телеком, 2000.
4. Расторгуев С.П. Программные методы защиты информации в компьютерах и сетях. М.: Яхтсмен, 1993. 188 с.
5. Брандман Э. Информационная безопасность российского общества в современных условиях [Электрон. ресурс] // Власть. 2007. № 5. С. 68–71. Режим доступа: [http://www.isras.ru/files/File/Vlast/2007/05/Informacionnaya\\_bezopasnost.pdf](http://www.isras.ru/files/File/Vlast/2007/05/Informacionnaya_bezopasnost.pdf).
6. Гафарова Г.Г., Смелянская В.В. Информационная безопасность личности [Электрон. ресурс] // Безопасность личности: состояние и возможности обеспечения. Материалы конференции. Пенза: Социосфера, 2012. Режим доступа: <http://sociosphera.com/publication/conference/2012/140/>.
7. Белякова Е.Г., Загвязинская Э.В., Березенцева А.И. Информационная культура и информационная безопасность школьников // Образование и наука. 2017. Т. 19. № 8. С. 147–162.
8. Аров Х.Н., Денщикова Т.Ю., Должикова М.В., Глущенко И.А., Петьков В.А. Технология обучения школьников основам информационной безопасности // Вестник АГУ. 2017. № 4(2008). С. 117–123.
9. Старков А.Н., Доколин А.С. Использование метода проектов для предупреждения киберэкстремистских идей среди молодежи // Управленческие механизмы противодействия идеологии экстремизма и терроризма. Материалы научно-практической конференции. Магнитогорск: Магнитогорский государственный технический университет им. Г.И. Носова, 2018. С. 112–116.
10. Кузнецова В.Ю. Обеспечение компетентности российских школьников в вопросах криптографии: анализ целей, возможных подходов и технологий, средств программной поддержки // Прикаспийский журнал: управление и высокие технологии. 2019. № 2(46). С. 163–170.
11. Петрова С.О. Этические подходы к информационной безопасности школьников в условиях электронного обучения // Вестник Государственного гуманитарно-технологического университета. 2021. № 3. С. 27–32.
12. Колесникова А.К., Пшеничная О.В., Чернова Е.В. Геймификация: использование игровой механики для обучения школьников основам безопасности в сети Интернет [Электрон. ресурс] // Научно-методический электронный журнал «Концепт». 2020. № 6. Режим доступа: <http://e-koncept.ru/2020/201044.htm>.
13. Карманова Е.В., Старков А.Н., Викулина В.В. Возможности применения технологии геймификации при реализации электронного обучения в вузе // Перспективы науки и образования. 2019. № 4(40). С. 462–472. DOI: 10.32744/pse.2019.4.35.
14. Romanova M.V., Romanov E.P., Varfolomeeva T.N., Lomakina E.A., Chernova E.V., Ruban K.A. Intellectual Game Application for Students' Knowledge Control [Электрон. ресурс] // Proceedings of the 2016 Conference on Information Technologies in Science, Management, Social Sphere and Medicine (ITSMSM 2016). С. 298–302. Режим доступа: [http://www.atlantispress.com/php/download\\_paper.php](http://www.atlantispress.com/php/download_paper.php).

15. Волкова В.Н., Денисов А.А. Основы теории систем и системного анализа. СПб.: СПбГТУ, 2001. 512 с.

16. Монахов С.В., Савиных В.П., Цветков В.Я. Методология анализа и проектирования сложных систем. М.: Просвещение, 2005. 264 с.

17. Зимняя И.А. Общая культура и социально-профессиональная компетентность человека [Электрон. ресурс] // Эйдос. 2006. Режим доступа: <http://www.eidos.ru/journal/2006/0504.htm>.

18. Хуторской А.В. Ключевые компетенции как компонент личностно-ориентированной парадигмы образования // Народное образование. 2003. № 2(1325). С. 58–64.

19. Бочаров М.И., Симонова И.В. Методика обучения информационной безопасности старшеклассников // Пространство и Время. 2013. № 4(14). С. 237–244.

20. Ковалева Н.Н. Информационное право России: учеб. пособие. М.: Издательско-торговая корпорация «Дашков и К», 2007.

21. Шалилова Ш.Т. Технология конструирования ситуационных задач в содержании прак-

тического обучения // Отечественная и зарубежная педагогика. 2012. № 2(5). С. 142–148.

22. Васева Е.С. Применение ситуационных задач в обучении старшеклассников информационной безопасности // Вопросы педагогики. 2020. № 8(2). С. 20–23.

23. Олейник Ю.П. Игрофикация в образовании: вопросы об определении понятия [Электрон. ресурс] // Современные проблемы науки и образования. 2015. № 3. Режим доступа: <https://science-education.ru/ru/article/view?id=20103>.

24. Дмитриев В.Л., Каримов Р.Х. Облачные технологии и игрофикация как основа научно-образовательной платформы для организации электронного обучения [Электрон. ресурс] // Профессиональное образование в России и за рубежом. 2016. № 2(22). Режим доступа: [http://www.prof-obr42.ru/Archives/2\(22\)2016.pdf](http://www.prof-obr42.ru/Archives/2(22)2016.pdf).

25. Каримов Р.Ж. Использование принципа игрофикации при организации электронного обучения // Электронное обучение в непрерывном образовании. Сборник научных трудов. Ульяновск: УлГТУ, 2015. С. 68–73.

## References

1. Rybakova O. S. Legislative regulation of ensuring the safety of the child in the Internet space. *Pravovaya informatika = Legal informatics*. 2017; 4: 49–54. (In Russ.)

2. Petrov V.P., Petrov S.V. *Informatsionnaya bezopasnost' cheloveka i obshchestva: uchebnoye posobiye = Information security of a person and society: a tutorial*. Moscow: ENAS; 2007. (In Russ.)

3. Zegzhda D.P., Ivashko A.M. *Osnovy bezopasnosti informatsionnykh system = Fundamentals of information systems security*. Moscow: Hotline-Telecom; 2000. (In Russ.)

4. Rastorguyev S.P. *Programmnyye metody zashchity informatsii v komp'yuterakh i setyakh = Software methods for protecting information in computers and networks*. Moscow: Yachtsman; 1993. 188 p. (In Russ.)

5. Brandman E. Information security of the Russian society in modern conditions [Internet]. *Vlast' = Power*. 2007; 5: 68–71. Available from: [http://www.isras.ru/files/File/Vlast/2007/05/Informacionnaya\\_bezopasnost.pdf](http://www.isras.ru/files/File/Vlast/2007/05/Informacionnaya_bezopasnost.pdf). (In Russ.)

6. Gafarova G.G., Smelyanskaya V.V. Information security of the individual [Internet]. *Bezopasnost' lichnosti: sostoyaniye i vozmozhnosti obespecheniya. Materialy konferentsii = Security of the individual: state and possibilities of provision. Conference materials*. Penza: Sociosfera; 2012. Available from: <http://sociosfera.com/publication/conference/2012/140/>. (In Russ.)

7. Belyakova Ye.G., Zagvyazinskaya E.V., Berezentseva A.I. Information culture and information security of schoolchildren. *Education and science*. 2017; 19; 8: 147–162. (In Russ.)

8. Arov Kh.N., Denshchikova T.Yu., Dolzhikova M.V., Glushchenko I.A., Pet'kov V.A. Technology of teaching schoolchildren the basics of information security. *Vestnik AGU = Bulletin of ASU*. 2017; 4(2008): 117–123. (In Russ.)

9. Starkov A.N., Dokolin A.S. Using the project method to prevent cyber-extremist ideas among young people. *Upravlencheskiye mekhanizmy protivodeystviya ideologii ekstremizma i terrorizma. Materialy nauchno-prakticheskoy konferentsii = Management mechanisms for countering the ideology of extremism and terrorism. Materials of the scientific-practical conference*. Magnitogorsk: Magnitogorsk State technical university G.I. Nosova; 2018: 112–116. (In Russ.)

10. Kuznetsova V.Yu. Ensuring the competence of Russian schoolchildren in matters of cryptography: analysis of goals, possible approaches and technologies, means of software support. *Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii = Caspian Journal: Management and High Technologies*. 2019; 2(46): 163–170. (In Russ.)

11. Petrova S.O. Ethical approaches to the information security of schoolchildren in the conditions of e-learning. *Vestnik Gosudarstvennogo gumanitarno-tekhnologicheskogo universiteta = Bulletin of the State Humanitarian and Technological University*. 2021; 3: 27–32. (In Russ.)

12. Kolesnikova A.K., Pshenichnaya O.V., Chernova Ye.V. Gamification: the use of game mechanics for teaching schoolchildren the basics of security on the Internet [Internet]. *Nauchno-metodicheskiy elektronnyy zhurnal «Kontsept» = Scientific and methodological electronic journal «Concept»*. 2020; 6. Available from: <http://e-koncept.ru/2020/201044.htm>. (In Russ.)

13. Karmanova, Ye.V., Starkov, A.N., Vikulina, V.V. Possibilities of using gamification technology in the implementation of e-learning at the university. *Perspektivy nauki i obrazovaniya* = Prospects of science and education. 2019; 4(40): 462-472. DOI: 10.32744/pse.2019.4.35. (In Russ.)

14. Romanova M.V., Romanov E.P., Varfolomeeva T.N., Lomakina E.A., Chernova E.V., Ruban K.A. Intellectual Game Application for Students' Knowledge Control [Internet]. Proceedings of the 2016 Conference on Information Technologies in Science, Management, Social Sphere and Medicine (ITSMSSM 2016). 2016: 298-302. Available from: [http://www.atlantis-press.com/php/download\\_paper.php](http://www.atlantis-press.com/php/download_paper.php).

15. Volkova V.N., Denisov A.A. *Osnovy teorii sistem i sistemnogo analiza* = Fundamentals of systems theory and system analysis. Saint Petersburg: SPbGTU; 2001. 512 p. (In Russ.)

16. Monakhov S.V., Savinykh V.P., Tsvetkov V.Ya. *Metodologiya analiza i proyektirovaniya slozhnykh sistem* = Methodology of analysis and design of complex systems. Moscow: Education; 2005. 264 p. (In Russ.)

17. Zimnyaya I.A. General culture and socio-professional competence of a person [Internet]. *Eidos*. 2006. Available from: <http://www.eidos.ru/journal/2006/0504.htm>. (In Russ.)

18. Khutorskoy A.V. Key competencies as a component of the personality-oriented paradigm of education. *Narodnoye obrazovaniye* = Public education. 2003; 2(1325): 58-64. (In Russ.)

19. Bocharov M.I., Simonova I.V. Methodology for teaching information security to high school

students. *Prostranstvo i Vremya* = Space and Time. 2013; 4(14): 237-244. (In Russ.)

20. Kovaleva N.N. *Informatsionnoye pravo Rossii: ucheb. Posobiye* = Information law of Russia: textbook. allowance. Moscow: Publishing and Trade Corporation «Dashkov and K»; 2007. (In Russ.)

21. Shalilova Sh.T. Technology for constructing situational problems in the content of practical training. *Otechestvennaya i zarubezhnaya pedagogika* = Domestic and foreign pedagogy. 2012; 2(5): 142-148. (In Russ.)

22. Vaseva Ye.S. Application of situational tasks in teaching high school students of information security. *Voprosy pedagogiki* = Questions of Pedagogy. 2020; 8(2): 20-23. (In Russ.)

23. Oleynik Yu.P. Gamification in education: questions about the definition of the concept [Internet]. *Sovremennyye problemy nauki i obrazovaniya* = Modern problems of science and education. 2015: 3. Available from: <https://science-education.ru/ru/article/view?id=20103>. (In Russ.)

24. Dmitriyev V.L., Karimov R.KH. Cloud technologies and gamification as the basis of a scientific and educational platform for organizing e-learning [Internet]. *Professional'noye obrazovaniye v Rossii i za rubezhom* = Vocational education in Russia and abroad. 2016: 2(22). Available from: [http://www.prof-obr42.ru/Archives/2\(22\)2016.pdf](http://www.prof-obr42.ru/Archives/2(22)2016.pdf). (In Russ.)

25. Karimov R.Zh. Using the principle of gamification in the organization of e-learning. *Elektronnoye obucheniye v nepreryvnom obrazovanii. Sbornik nauchnykh trudov* = E-learning in lifelong education. Collection of scientific papers. Ulyanovsk: UIGTU; 2015: 68-73. (In Russ.)

## Сведения об авторах

**Марина Викторовна Романова**

К.п.н., доцент, доцент кафедры  
Бизнес-информатики и информационных  
технологий

Магнитогорский государственный технический  
университет им. Г.И. Носова

Магнитогорск, Россия

Эл. почта: [romanova.mv@mail.ru](mailto:romanova.mv@mail.ru)

**Елена Владимировна Чернова**

К.п.н., доцент, доцент кафедры  
Бизнес-информатики и информационных  
технологий

Магнитогорский государственный технический  
университет им. Г.И. Носова

Магнитогорск, Россия

Эл. почта: [ev.chernova@magtu.ru](mailto:ev.chernova@magtu.ru)

## Information about the authors

**Marina V. Romanova**

Cand. Sci. (Pedagogical), Associate Professor,  
Associate Professor of the Department of Business  
Informatics and Information Technologies  
Magnitogorsk State Technical University named after  
G.I. Nosov

Magnitogorsk, Russia

E-mail: [romanova.mv@mail.ru](mailto:romanova.mv@mail.ru)

**Elena V. Chernova**

Cand. Sci. (Pedagogical), Associate Professor,  
Associate Professor of the Department of Business  
Informatics and Information Technologies  
Magnitogorsk State Technical University named after  
G.I. Nosov

Magnitogorsk, Russia

E-mail: [ev.chernova@magtu.ru](mailto:ev.chernova@magtu.ru)