УДК 371
ББК 74.409

Е. Ю. Огурцова, Р. Н. Фадеев

ПОДГОТОВКА БУДУЩИХ УЧИТЕЛЕЙ К ОБУЧЕНИЮ ШКОЛЬНИКОВ ОСНОВАМ КИБЕРБЕЗОПАСНОСТИ

В статье рассматривается проблема подготовки педагогических кадров, способных на высоком профессиональном уровне помочь детям освоить основы кибербезопасности. Рассказано об опыте подготовки будущих педагогов в рамках курса «Основы кибербезопасности». Особое внимание уделяется интерактивным методам, которые можно применить в работе со студентами. Отмечается, что полученный при этом опыт будущие учителя могут использовать при организации занятий для развития у школьников навыков поведения в цифровом мире. Подчеркивается, что использование учебно-методических задач при подготовке студентов позволяет осуществить моделирование в учебной деятельности аспектов будущей просветительской работы в области информационной безопасности. Сделан вывод, что содержание данного курса, применяемые формы и методы обучения студентов позволяют сформировать у будущих педагогов готовность к обучению школьников основам кибербезопасности.

Ключевые слова: педагогическая деятельность, основы кибербезопасности, школьники в цифровом пространстве, интерактивные методы.

E. Yu. Ogurtsova, R. N. Fadeev

PREPARING FUTURE TEACHERS TO TEACH SCHOOL PUPILS THE BASICS OF CYBERSECURITY

The article discusses the problem of training pedagogical personnel capable at a high professional level of helping children to master the basics of cybersecurity. The experience of training future teachers in the framework of the course «Basics of Cybersecurity» is described. Particular attention in the article is paid to interactive methods that can be applied to work with students. It is noted that future teachers can use the experience gained at the same time when organizing classes to develop students' skills of behavior in the digital world. It is emphasized that the use of educational and methodological tasks in the preparation of students allows modeling in learning activities aspects of future educational work in the field of information security. It is concluded that the content of this course, the forms and methods of teaching students used, make it possible to form in future teachers a readiness to teach schoolchildren the basics of cybersecurity.

Key words: pedagogical activity, basics of cybersecurity, schoolchildren in the digital space, interactive methods.

DOI: 10.46724/NOOS.2021.3.88-97

Ссылка для цитирования: Огурцова Е. Ю., Фадеев Р. Н. Подготовка будущих учителей к обучению школьников основам кибербезопасности // Ноосферные исследования. 2021. Вып. 3. С. 88—97.

Citation Link: Ogurtsova, E. Yu., Fadeev, R. N. (2021) Podgotovka budushchih uchitelej k obucheniyu shkol'nikov osnovam kiberbezopasnosti [Preparing future teachers to teach school pupils the basics of cybersecurity], *Noosfernyye issledovaniya* [*Noospheric Studies*], vol. 3, pp. 88—97.

Актуальность проблематики информационной безопасности обусловлена синергетическим эффектом, определяемым двумя факторами:

- резкий рост компьютерных вторжений, основанных на методах социальной инженерии;
- карантинные мероприятия, реализующие современные возможности удаленной работы, что изменило устоявшиеся режимы безопасного и устойчивого функционирования систем в Интернете.

При распространении новой коронавирусной инфекции в марте 2020 года в соответствии с рекомендациями Министерства просвещения Российской Федерации (приказ № 104 от 17.03.2020) в целях обеспечения безопасности обучающихся и педагогических работников школам было предложено организовать взаимодействие участников образовательного процесса опосредованно (на расстоянии).

В условиях самоизоляции на смену традиционному пришли различные формы дистанционного обучения. В информационное пространство вышли даже те педагоги, школьники и их родители, которых до пандемии там не было или их присутствие было ограничено. Возникали угрозы устойчивого функционирования интернет-сети, например, было периодическое зависание портала Учи.ру. Отмечается, что хакерские атаки на школьные видеоконференции носили массовый характер. Обучение различных слоев населения нашей страны основам кибербезопасности стало весьма актуальным.

Шквал сетевых опасностей обрушивается на детей, которые в силу возраста, отсутствия знаний или опыта не всегда могут им противостоять. Исследователи из Северного (Арктического) федерального университета имени М. В. Ломоносова выявили, что современные школьники не придают значения факту наличия интернет-преступников, совершающих мошеннические действия [5, 6]. Основная роль в киберобразовании отводится школе. В профессиональном стандарте педагога указано, что каждый учитель должен уметь формировать и реализовывать программы развития у обучающихся навыков поведения в мире виртуальной реальности и социальных сетях. Учителя, работая в единой команде, могут научить детей правильно и безопасно вести себя в цифровом пространстве.

Необходимы педагогические кадры, заинтересованные и способные методически грамотно научить школьников «цифровой гигиене» — правилам поведения в цифровой среде. Вузы должны принимать активное участие в процессе подготовки будущих учителей, способных на высоком профессиональном уровне объяснить детям основы кибербезопасности. По нашему мнению, заинтересованными сторонами в организации такой подготовки являются непосредственно студенты и опосредованно вуз. Студентам это необходимо для формирования опыта просветительской работы в области информационной

безопасности, эффективной, успешной профессиональной деятельности в дальнейшем, а вузу — для повышения конкурентоспособности на рынке образовательных услуг и обеспечения качества образования.

Однако анализ учебных планов для педагогических направлений подготовки показал, что в них нет курсов, направленных на формирование у студентов методических умений и навыков для обучения школьников основам кибербезопасности [1].

Для студентов направления подготовки 44.04.01 Педагогическое образование (профиль образовательной программы «Информационные технологии в профессиональной деятельности педагога») в Шуйском филиале Ивановского государственного университета с целью создания условий для развития у будущих педагогов специальных компетенций предусмотрен курс «Основы кибербезопасности», в рамках которого обучение идет в двух направлениях:

- изучение основ кибербезопасности (риски работы в киберпространстве, виды информационных угроз, средства и методы борьбы с киберугрозами, защита персональной информации, двухфакторная аутентификация, системный подход против социальной инженерии и т. д.);
- рассмотрение педагогических сценариев обучения школьников и их родителей основам кибербезопасности.

В начале курса большое внимание уделяется формированию мотивации у студентов. Рассматривая статистические данные и конкретные примеры, мы стараемся убедить студентов, что киберугрозы — это реальная опасность. Большое количество современных учеников сталкиваются с киберугрозами в повседневной жизни, и один из способов защитить их — образование в области кибербезопасности. Вы — будущие учителя, и у вас есть уникальная возможность повлиять на будущее поколение и научить своих учеников правильно реагировать на соответствующие проблемы.

Для будущих педагогов в рамках данного курса нами разработана система учебно-методических задач, использование которых при подготовке студентов позволяет осуществить моделирование в учебной деятельности аспектов будущей профессиональной деятельности [2]. В систему входят различные виды учебно-методических задач. Рассмотрим в качестве примера некоторые из них.

- Вам необходимо провести классный час для обучающихся и родительское собрание, посвященные проблеме обеспечения кибербезопасности. Составьте список вопросов, которые вы будете обсуждать с детьми на классном часе. Составьте список вопросов, которые вы будете рассматривать с родителями на собрании. Укажите основное отличие при формировании этих списков. Ответ обоснуйте.
- Создайте постер, посвященный какому-либо аспекту кибербезопасности.
- Разработайте сценарий квеста по теме «Киберугрозы». Объясните свой отбор материала для него.
- Вам предстоит провести ролевую игру в 8 классе «Риски работы в киберпространстве». Опишите роли, предлагаемые обучаемым (например, Сетевой геймер, Веб-клиент, Виртуальный собеседник и т. п.). Предложите задания для каждой роли.

• Вы с младшими школьниками создаете «Дерево безопасности в цифровом пространстве». Оно имеет зеленые, желтые и красные листья. Зеленые листья — на них размещаем то, что можно и нужно делать в указанном пространстве; желтые — нужно проявлять осторожность; красные — делать ни в коем случае нельзя. Спланируйте свою беседу с учениками во время этой совместной работы.

• Представьте, что необходимо выбрать организационную форму для обучения учащихся 5 класса безопасной работе в социальных сетях. Какую форму вы предпочтете? Докажите правильность вашего выбора с теоретической точки зрения.

• Составьте список лучших с вашей точки зрения сайтов, посвященных защите от вредоносного программного обеспечения, которые вы могли бы порекомендовать ученикам. Дате краткую аннотацию каждого сайта из списка.

• Разработайте онлайн-опрос, который позволит вам оценить общий уровень знаний учеников по теме «Защита от фишинга».

• Чтобы помочь вашим ученикам понять последствия, связанные с кибератаками, их масштаб и серьезность, вы хотите познакомить их с историями людей и организаций, ставших жертвами кибератак**.** Приведите примеры несколько историй, которые можно было бы использовать.

• Подготовьте инструкцию для обучающихся «Меры предосторожности при работе с публичными точками доступа Wi-Fi».

• Составьте краткий словарь кибербуллинга. Объясните значение терминов: троллинг, флейминг, харрасмент, киберсталкинг, кэтфишинг, фрейпинг, грифинг, аутинг, распекание. Опишите возможные способы использования педагогом сведений из данного словаря.

• Подготовьте аудиоматериал на тему «Незнакомцы из киберпространства». Используйте подкаст для размещения своего аудиофрагмента.

• Подберите цитату, эпиграф или девиз, которые кратко характеризуют один из аспектов кибербезопасности.

• Выделите ключевые слова темы «Безопасность в социальных сетях». Для их визуального представления создайте облако слов. Используйте для этого цифровой сервис.

Студенты пишут диктант по кибербезопасности, который проходит в форме теста и состоит из двух частей. Первая составлена из 15 вопросов базового уровня («ликбез по кибербезопасности»), вторая рассчитана на применение методических умений будущих учителей.

При работе со студентами мы стремимся использовать интерактивные методы. Опыт, полученный в ходе таких занятий, студенты смогут использовать при организации урочной и внеурочной деятельности школьников с целью знакомства с основами кибербезопасности.

На одном из занятий прошли дебаты на тему «Береги онлайн-репутацию смолоду». При предварительной подготовке студентам необходимо было ясно и логично сформулировать свою позицию; найти убедительные факты и доводы в свою поддержку; предсказать, какими будут доводы противной стороны, и подготовить контраргументы.

Студенты разрабатывали практико-ориентированные проекты, связанные с социальной рекламой «Как ты можешь противостоять киберугрозе». Препода-

ватель при выполнении этих проектов выступал как консультант и эксперт, его главная функция — поддержать студента в его деятельности, помочь структурировать, освоить большую и разнообразную информацию, облегчить решение возникающих при этом проблем.

Особое внимание при работе со студентами уделяем составлению и решению ситуационных задач, позволяющих сочетать компетентностно-ориентированный подход с традиционным содержанием образования [4]. Ситуационные задачи являются эффективными инструментами для подготовки обучающихся к распознаванию киберугроз и правильному поведению при встрече с ними. Рассмотрим некоторые из них:

• Коля, возвращаясь из школы домой, нашел флешку. Дома он решил посмотреть, какая информация на ней хранится. Мальчик вставил флешку в ноутбук. Неожиданно тот начал перезагрузку, а когда включился, то на рабочем столе исчезли все ярлыки. Что могло произойти? Как правильно было действовать в данной ситуации?

• Вы получили следующее электронное письмо.

«Здравствуйте [имя], мы сожалеем, но ваша учетная запись была заблокирована. Чтобы восстановить учетную запись, пожалуйста, откройте файл netaccountinformation.exe и укажите следующие данные:

Ваше полное имя.

Ваша дата рождения.

Ваш адрес.

Ваш номер телефона.

С уважением, служба работы с клиентами»

Стали бы Вы отвечать на такое сообщение или нет? Почему приняли такое решение?

• Учитель опубликовал в соцсетях ссылку на Zoom-конференцию, приглашая к участию учеников. Как вы считаете, нарушил он правила кибербезопасности или нет? Ответ обоснуйте.

• Саше на телефон пришло СМС-сообщение: «Доброго времени суток! По вашим паспортным данным найдены страховые начисления в размере 4789 руб. Подробности на сайте: http://snils.online». Он перешел по ссылке. Какие ошибки допустил Саша? Какие последствия могут возникнуть в результате его действий? Обоснуйте свой ответ. Составьте рекомендации, в которых будет содержаться описание признаков смс-мошенничества и правил поведения при встрече с ним.

В своей работе мы попробовали использовать современный игровой формат под названием «Конференция провалов». Совершение ошибок — интегральное свойство человеческой природы. И чем больше и сложнее тема, тем больше ошибок можно совершить, а кибербезопасность — тема с множеством факторов, которые необходимо брать во внимание. На публичных мероприятиях обычно рассказывают об успешных проектах и победах, а ошибки, провалы и неудачи принято держать в секрете. Но каждая неудача — это бесценный опыт, которым надо обязательно поделиться с другими. На этом интерактивном мероприятии будущие педагоги имели возможность рассказать о своих провалах и вынесенных из этого уроках. Данный формат работы предполагает использование технологии сторителлинга.

Термин «сторителлинг» заимствован из английского языка и переводится как «рассказывание историй». Ввел данный термин Дэвид Армстронг, глава международной компании Armstrong International. Разрабатывая свой метод, он учел психологические особенности восприятия, внимания, памяти: истории более выразительны, интересны и легче ассоциируются с личным опытом, чем правила. Использование данной технологии предполагает создание историй с определенной структурой [3]. Важно, чтобы слушатели поверили рассказчику, начали сопереживать.

«Сессия позади, впереди целая неделя каникул. Самое время заняться шопингом. Гуляя по торговому центру, я увидела платье, которое мне очень понравилось. Оно просто шикарное, эффектное. Примерила его. Как оно мне идет! Я в нем просто красотка, но его цена… Это же несколько моих стипендий. В голову пришла мысль проверить, сколько похожее платье стоит в интернет-магазине. Не задумываясь, я подключилась к одной из обнаруженных открытых сетей «FreeWiFi». Зайдя на сайт интернет-магазина, нашла точно такое же платье моего размера, но по цене в 3 раза дешевле. Ура! Ура! Ура! Тут же оформляю онлайн-покупку, введя номер банковской карты и трехзначный код с ее обратной стороны. Жаль, подружка уехала к себе домой на каникулы. Ну да ладно, поделюсь с ней своей радостной новостью через социальную сеть…»

Приведенный выше фрагмент рассказа по своему содержанию можно было бы уместить в короткую фразу: «Через общественную сеть Wi-Fi передала конфиденциальные данные». Разница между двумя описаниями заключается в том, что первое позволяет слушателю пережить рассказанный опыт. Тогда как второе просто констатирует факт.

В процессе формирования профессиональных компетенций будущих учителей мы применяем моделирование фрагмента внеурочного занятия со школьниками. Один из студентов группы выступает в роли учителя, остальные – ученики. Например, после рассказа о характерных признаках фишингового электронного письма студенты в качестве учеников выполняют упражнение: написать фишинговые письма с целью узнать личные данные получателя письма. Студент, исполняющий функции учителя, должен проанализировать работы студентов-учеников, выбрать самые убедительные, зачитать их и объяснить, почему он считает, что это удачные наглядные примеры фишинговых писем.

Еще одна из форм работы со студентами, которую они впоследствии могут реализовать в процессе обучения школьников, — конкурс комиксов по основам кибербезопасности. Главное при создании комикса — придумать историю и спланировать череду событий. Для визуализации сюжета можно воспользоваться цифровыми сервисами (рис. 1).

Важную роль в курсе играет знакомство студентов с сайтами и порталами, которые предлагают актуальную информацию для обучающихся и их родителей по основам безопасного поведения в киберпространстве, предоставляют методическую поддержку для учителей (рекомендации и видеоматериалы к уроку «Безопасность будущего»; запись вебинара для учителей и директоров школ, который проводил руководитель направления «Лаборатории Касперского» по защите детей в Интернете; конспекты уроков учителей по данной тематике и т. д.).

Рис. 1. Фрагмент комикса, созданного с помощью цифрового сервиса

Тренажер урока «Безопасность будущего» включает в себя три варианта сценариев с тремя разными героями − биологом, художником и математиком. Школьник может выбрать персонажа, за которого хочет играть, а после пройти урок еще раз − за другого героя. Каждому из них нужно достичь определенной цели, а для этого выполнить ряд действий. Задания внутри сценариев направлены на знакомство с темой безопасности при помощи ситуаций, с которыми дети могут столкнуться и в реальной жизни. После завершения игры школьникам будет предложено пройти финальный тест. Задания, предлагаемые в тренажере, различаются для младшей, средней и старшей школы.

Портал «Безопасность детей в сети» (https://kids.kaspersky.ru/) рассказывает ребятам, с какими угрозами они могут столкнуться в Интернете и как избежать неприятностей, а родители узнают, как помочь детям осваивать цифровой мир безопасно. Для учителей на сайте доступны методические материалы для школьных уроков по информационной безопасности. На портале представлены два анимационных сериала: о приключениях мальчика Севы и робота Каспера на просторах Интернета и «Фикси-советы. Осторожней в Интернете!». В сериях Каспер расскажет про кибербуллинг, фишинг, приватность аккаунтов, пиратских сайтах, покупках в компьютерных играх и многом другом в области кибербезопасности (рис. 2). Фиксики в занимательной форме дадут советы по безопасности в Интернете (рис. 3).

На «Уроке цифры» по теме «Приватность в цифровом мире» (https://урокцифры.рф/lessons/cybersecurity/materials) ученики смогут познакомиться с основами информационной безопасности и развивать важное в XXI веке умение – защищать свои персональные данные. На уроке идет работа по формированию таких понятий, как персональные данные, приватность, конфиденциальность, овершеринг, цифровой след и шпионское программное обеспечение. Онлайн-тренажеры для учеников 1—11 классов помогут закрепить данные понятия в игровой форме. Настройки прохождения в тренажере позволяют выбрать опции: ученик, учитель, родитель.

Рис. 2. Фрагмент серии про кибербуллинг

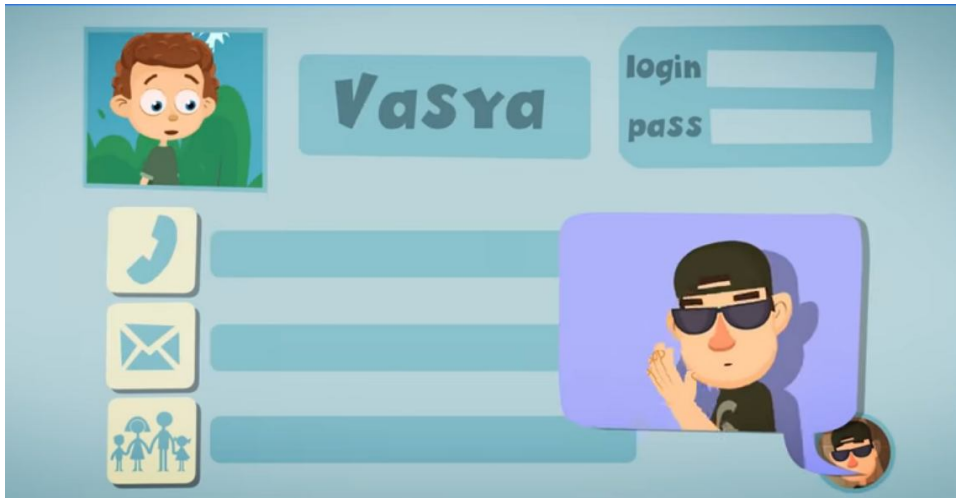

Рис. 3. Фрагмент серии мультфильма «Фикси-советы. Осторожней в Интернете!»

Резюмируя вышесказанное, можно отметить, что содержание данного курса, применяемые нами в рамках курса формы и методы обучения студентов позволяют сформировать у будущих педагогов готовность к обучению школьников основам кибербезопасности. Целенаправленное формирование у студентов опыта использования различных средств, методов, приемов и организационных форм обучения безопасному поведению в цифровом пространстве помогает им успешно осуществлять подобную педагогическую деятельность в дальнейшей работе со школьниками.

Библиографический список

1. *Богатырева Ю. И.* Методическая система подготовки будущих педагогов к обеспечению информационной безопасности школьников // Современные проблемы науки и образования: электронный научный журнал. 2014. № 1. URL: http://science-education.ru/ru/article/view?id=11957 (дата обращения: 11.05.2021).

2. *Огурцова Е. Ю.* Учебно-методические задачи как средство формирования у будущих педагогов профессиональных умений по использованию сервисов Веб 2.0 // Современные технологии в науке и образовании: сборник трудов Международного научно-технического форума: в 11 т. / под ред. О. В. Миловзорова. Рязань, 28 февраля — 2 марта 2018 г. Т. 9. Рязань: Рязан. гос. радиотехн. ун-т; Book Jet, 2018. С. 61—64.

3. *Огурцова Е. Ю.*, *Журавлев И. Д.* Использование цифрового сторителлинга в профессиональной деятельности педагога // Ученые записки ИУО РАО. 2017. № 1 (61). С. 111—113.

4. *Суровцева В. А.* Ситуационная задача как один из современных методических ресурсов обновления содержания школьного образования // Школьная педагогика. 2016. № 4 (7). С. 48—57.

5. *Троицкая О. Н.*, *Вохтомина Е. Д.* Подготовка будущих учителей математики и информатики к обучению школьников основам кибербезопасности // Информатика и образование. 2019. № 8. С. 24—31.

6. *Троицкая О. Н.*, *Ширикова Т. С.*, *Безумова О. Л.*, *Лыткина Е. А.* Концептуальная модель обучения основам кибербезопасности в основной школе // Современные проблемы науки и образования: электронный научный журнал. 2018. № 5. URL: https://science-education.ru/ru/article/view?id=28073 (дата обращения: 11.05.2021).

References

Bogatyreva, Yu. I. (2014) Metodicheskaja sistema podgotovki budushhih pedagogov k obespecheniju informacionnoj bezopasnosti shkol'nikov [Methodological system of training future teachers to ensure information security of schoolchildren], *Sovremennye problemy nauki i obrazovanija: jelektronnyj nauchnyj zhurnal* [Modern problems of science and education: electronic scientific journal], no. 1. URL: http://science-education.ru/ru/article/view?id=11957 (data obrashhenija: 11.05.2021).

Ogurtsova, E. Yu. (2018) Uchebno-metodicheskiye zadachi kak sredstvo formirovaniya u budushchikh pedagogov professional'nykh umeniy po ispol'zovaniyu servisov Veb 2.0 [Educational and methodological tasks as a means of developing professional skills in the use of Web 2.0 services in future teachers], in Milovzorov, O. V. (ed.) *Sovremennyye tekhnologii v nauke i obrazovanii* [Modern technologies in science and education: collection of works of the international scientific and technical forum], vol. 9, Ryazan': Ryazanskiy gosudarstennyy radiotekhnicheskiy universitet; Book Jet, pp. 61—64.

Ogurcova, E. Yu., Zhuravlev, I. D. (2017) Ispol'zovanie cifrovogo storitellinga v professional'noj dejatel'nosti pedagoga [Using digital storytelling in teacher's professional activities], *Uchenye zapiski IUO RAO* [Scientists notes IU RAO], no. 1 (61), pp. 111—113.

Surovceva, V. A. (2016) Situacionnaja zadacha kak odin iz sovremennyh metodicheskih resursov obnovlenija soderzhanija shkol'nogo obrazovanija [Situational task as one of the modern methodological resources for updating the content of school education], *Shkol'naja pedagogika* [School pedagogy], no. 4 (7), pp. 48—57.

Troickaja, O. N., Vohtomina, E. D. (2019) Podgotovka budushhih uchitelej matematiki i informatiki k obucheniju shkol'nikov osnovam kiberbezopasnosti [Training future mathematics and computer science teachers to teach students the basics of cybersecurity], *Informatika i obrazovanie* [Informatics and Education], no. 8, pp. 24—31.

Troickaja, O. N., Shirikova, T. S., Bezumova, O. L., Lytkina, E. A. (2018) Konceptual'naja model' obuchenija osnovam kiberbezopasnosti v osnovnoj shkole [Basic School Cybersecurity Learning Conceptual Model], *Sovremennye problemy nauki i obrazovanija: jelektronnyj nauchnyj zhurnal* [Modern problems of science and education: electronic scientific journal], no. 5. URL: https://science-education.ru/ru/article/view?id=28073 (data obrashhenija: 11.05.2021).

Статья поступила в редакцию 31.05.2021 г.

Сведения об авторах

Огурцова Елена Юрьевна — кандидат педагогических наук, доцент, Ивановский государственный университет (Шуйский филиал), г. Шуя, Россия, ogurcova-elena@mail.ru

Фадеев Роман Николаевич — студент, Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, г. Владимир, Россия, fadeevroman.shua@gmail.com

Information about the authors

Ogurtsova Elena Yurievna — Cand. Sc. (Pedagogical), Associate Professor, Ivanovo State University (Shuya branch), Shuya, Russian Federation, ogurcova-elena@mail.ru

Fadeev Roman Nikolaevich — student, Vladimir State University named after Alexander Grigorievich and Nikolai Grigorievich Stoletovs, Vladimir, Russian Federation, fadeevroman.shua@gmail.com