

Г. Н. Чусавитина, Е. В. Карманова,

Магнитогорский государственный технический университет им. Г. И. Носова, Челябинская область

ИСПОЛЬЗОВАНИЕ СЕТЕВЫХ СЕРВИСОВ ВЕБ 2.0 ПРИ РЕАЛИЗАЦИИ ПРОЕКТНОГО ПОДХОДА В ОБУЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация

В статье описывается опыт повышения эффективности формирования компетентности студентов педагогического образования в области обеспечения информационной безопасности. Указано на необходимость не только совершенствования теоретического содержания преподаваемой дисциплины, но и разработки новых методических подходов к преподаванию основ информационной безопасности. Раскрываются приемы использования сетевых сервисов Веб 2.0 при организации учебных проектов, представлен обзор сервисов по категориям, а также предложены конкретные примеры их использования при организации проектной деятельности по теме информационной безопасности.

Ключевые слова: информационная безопасность, компетентность в области обеспечения информационной безопасности, сервисы Веб 2.0, метод проектов, ментальные карты, инфографика, учебные проекты, ленты времени, закладки.

В современном цифровом мире информационно-коммуникационные технологии настолько проникли в жизнь каждого человека, что порой уже невозможно определить и разграничить онлайн-ую и офлайн-ую деятельность. Использование мобильных устройств, планшетов, работа с электронной почтой, мессенджерами, социальными сетями стали неотъемлемым компонентом жизни современного человека.

Однако, несмотря на широкое распространение и использование ИКТ, уровень компетенции молодежи в сфере информационной безопасности остается недостаточно высоким. Несоблюдение политики конфиденциальности, размещение персональных данных в публичных сетях, доверие к ресурсам с подозрительным контентом, отсутствие надежных паролей — это всего лишь небольшой спектр проблем, с которыми сталкиваются пользователи ИКТ. Формирование компетенций в области информационной безопасности и защиты информации у студен-

тов, обучающихся по направлению «Педагогическое образование», является одной из актуальных проблем современного образования [3, 12–18, 21–25]. Необходимость повышения уровня грамотности, информационной культуры в сфере информационной безопасности представлена на законодательном уровне — в рамках государственных программ «Информационное общество» [1] и «Цифровая экономика» [10]. В данных документах предлагается ряд проектов по развитию системы получения знаний в сфере информационной безопасности на базе Национальной электронной библиотеки, а также платформы массовых онлайн-курсов. Однако остается проблема недостаточной проработанности методических подходов к преподаванию основ информационной безопасности.

Для решения данной проблемы мы предлагаем использовать в преподавании дисциплины «Информационная безопасность» метод проектов,

Контактная информация

Чусавитина Галина Николаевна, канд. пед. наук, профессор, зав. кафедрой бизнес-информатики и информационных технологий Магнитогорского государственного технического университета им. Г. И. Носова, Челябинская область; *адрес:* 455000, Челябинская обл., г. Магнитогорск, пр-т Ленина, д. 38; *телефон:* (3519) 29-85-85; *e-mail:* Gala_m27@mail.ru

Карманова Екатерина Владимировна, канд. пед. наук, доцент, доцент кафедры бизнес-информатики и информационных технологий Магнитогорского государственного технического университета им. Г. И. Носова, Челябинская область; *адрес:* 455000, Челябинская обл., г. Магнитогорск, пр-т Ленина, д. 38; *телефон:* (3519) 29-85-85; *e-mail:* monitor81@mail.ru

G. N. Chusavitina, E. V. Karmanova,

Nosov Magnitogorsk State Technical University, Chelyabinsk Region

USING WEB 2.0 SERVICES AT THE IMPLEMENTATION OF THE PROJECT APPROACH IN TEACHING INFORMATION SECURITY

Abstract

The article describes the experience of increasing the effectiveness of forming the competence of students of teacher education in the field of information security. It is pointed out that it is necessary not only to improve the theoretical content of the discipline, but also to develop new methodological approaches to teaching the basics of information security. Methods of using Web 2.0 networking services in the organization of training projects are described, an overview of services by category is provided, and specific examples of their use in organizing project activities on the theme of information security are offered.

Keywords: information security, competence in field of information security, Web 2.0 services, project method, mental maps, infographic, educational projects, timelines, bookmarks.

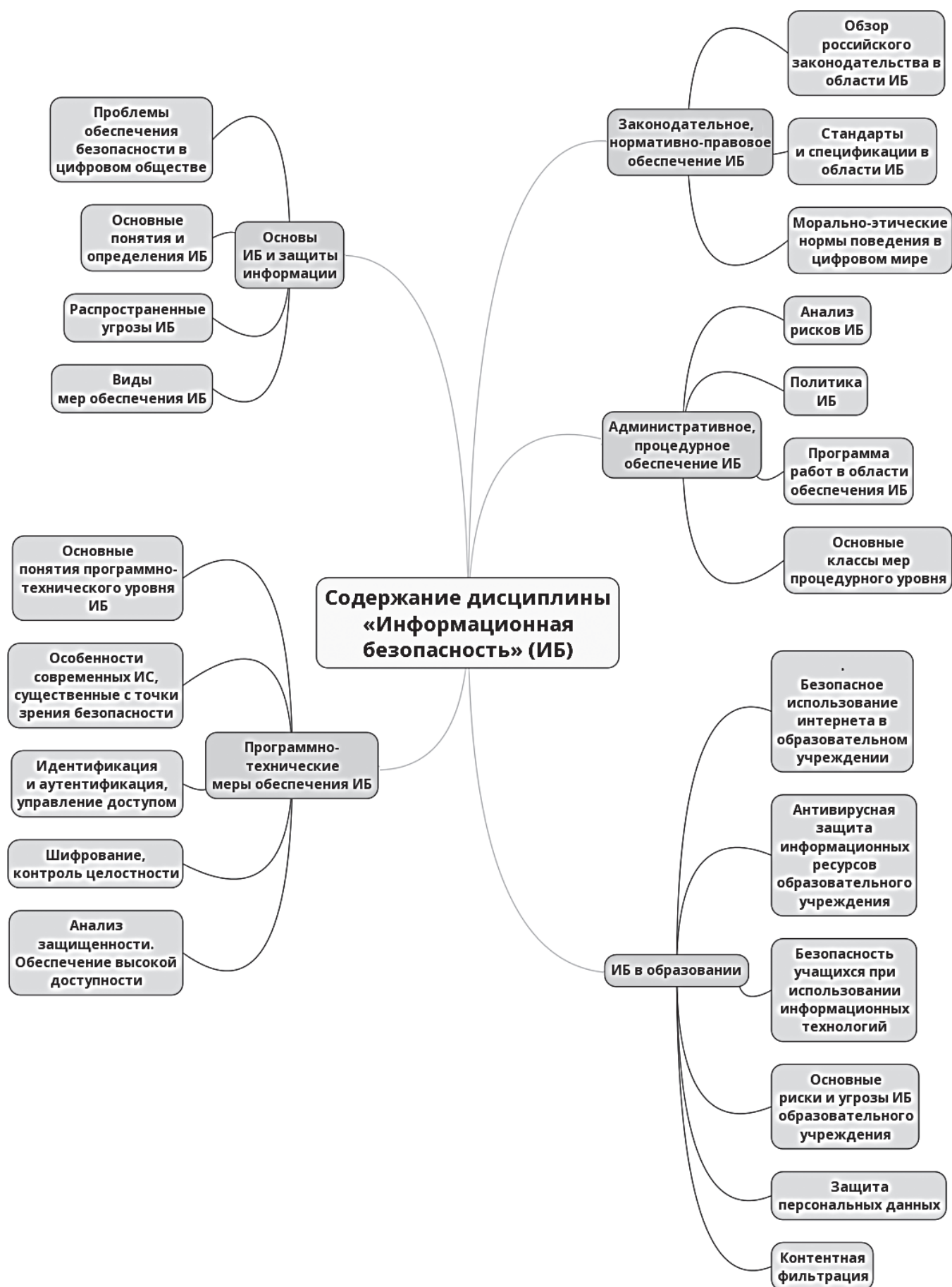


Рис. 1. Содержание дисциплины «Информационная безопасность» для бакалавров педагогического образования

который позволяет сочетать традиционные и инновационные методы обучения.

На рисунке 1 представлено основное содержание рабочей программы дисциплины «Информационная безопасность», разработанной в ФГБОУ ВО «Магнитогорский государственный технический университет им. Г. И. Носова» для бакалавров педагогического образования, а также приведено краткое содержание пяти разделов этой программы [16].

Выбор проектного подхода в качестве основного при преподавании дисциплины «Информационная безопасность» обусловлен известным положением, что продуктивность образования заметно возрастает в случае личной заинтересованности студента в результате проекта, участия в проекте нескольких заинтересованных лиц. В своей работе мы опирались на исследования, посвященные методологическим аспектам реализации метода проектов в образовании [4, 8, 9, 20]. В основе метода проектов лежит идея организации процесса обучения таким образом, чтобы студенты получали новые знания, формировали умения и навыки, приобретали опыт практической деятельности в процессе выполнения реальных проектов, которые должны завершиться некоторым реальным результатом.

Применение метода проектов в рамках преподавания информационной безопасности для будущих учителей обусловлено следующими обстоятельствами: студентам создаются условия, когда они изучают теорию и практику «на деле», самостоятельно конструируют знания, формируют умения, активно включаются в практическую деятельность при инициации, планировании, мониторинге и контроле, реализации и закрытии проекта в сфере информационной безопасности.

Представим темы проектов, реализуемых в рамках изучения дисциплины «Информационная безопасность» бакалаврами педагогического образования:

- арт-проекты:
 - плакат на тему «Защитим детей от кибербуллинга»;
 - плакат на тему «Как уберечься от кардинга*»;
 - комикс на тему «Когда тебя взломали»;
 - открытка на тему «С днем информационной безопасности»;
 - комикс на тему «Общение с флеймером**»;
 - карикатура на тему «Троллинг*** в сети»;
- образовательные проекты:
 - мастер-класс «Защита мобильного устройства»;
 - акция «Нет крэкингу****!»;

* Кардининг — использование чужой (ворованной) кредитной карты для оплаты товаров или услуг [12].

** Флейм — «спор ради спора», обмен сообщениями в местах многопользовательского сетевого обмена, представляющий собой войну, нередко уже не имеющую отношения к первоначальной причине спора [12].

*** Троллинг — нагнетание участником общения в компьютерной сети гнева, конфликта путем скрытого или явного задиранья, принижения, оскорбления другого участника или участников [12].

**** Крэкинг — взлом и изменение программ на свое усмотрение или на заказ [12].

- праздник в честь дня создания сети Интернет;
- круглый стол «Современные уязвимости в сфере информационной безопасности»;
- кейс реальной ситуации, которая могла произойти в сфере информационной безопасности;
- курс «Защита персональных данных»;
- исследовательские проекты:
 - проект «Когда настанет информационный взрыв?»;
 - проект «Последствия DDOS-атак»;
 - проект «Будущее цифровых денег. Информационная безопасность блокчейн»;
 - проект «Здоровье интернета»;
 - проект «Меры предупреждения угроз в сфере информационной безопасности»;
- технологические проекты:
 - разработка инфраструктуры информационной безопасности образовательного учреждения;
 - разработка политики и программы информационной безопасности «Цифровая и безопасная школа»;
 - технология защиты персональных данных и др.;
- программные проекты:
 - разработка (проектирование) обучающей программы по информационной безопасности;
 - разработка мобильного приложения для обеспечения информационной безопасности в беспроводных локальных сетях;
 - компьютерная игра «Шифр Энигма»;
 - чат-бот «Сетикет» и др.

В качестве информационно-коммуникационных технологий, применяемых при реализации проектов, было принято решение использовать сетевые сервисы Веб 2.0, которые позволяют повысить познавательный интерес студентов к проблематике учебной дисциплины, разнообразить основные виды деятельности в ходе выполнения проекта, представить проектные решения по проблемам информационной безопасности в наглядном, интерактивном виде.

На рисунке 2 представлены основные категории сервисов Веб 2.0, а также конкретные ресурсы, которые можно использовать педагогу при проведении занятий [2].

Рассмотрим подробнее **возможности использования сетевых сервисов Веб 2.0 при реализации образовательных проектов в рамках изучения информационной безопасности.**

Сервис создания комиксов — Pixton: <https://www.pixton.com/ru/>

Сервис содержит большую коллекцию готовых тематических шаблонов для создания комиксов (офис, город, магазин, домашняя обстановка, кафе, школа, университет и т. д.), также предлагаются готовые персонажи — люди, животные. В функционал входят возможность применения различных поз, эмоций для персонажей, реализация подписей для раскадровки, совместное редактирование комиксов и т. д.

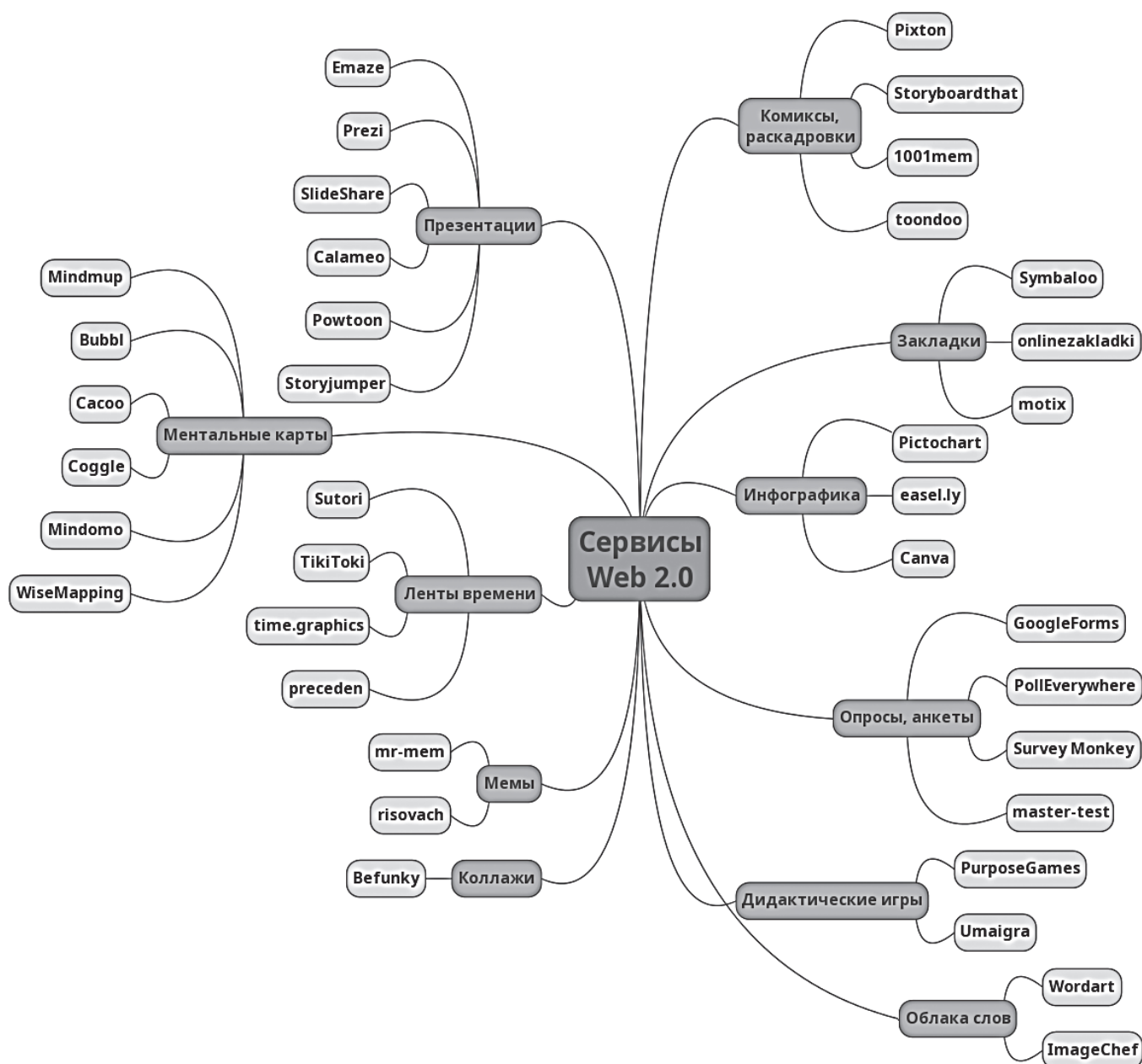


Рис. 2. Сетевые сервисы Веб 2.0

Данный сервис позволяет реализовать следующие педагогические возможности:

- построение диалогов;
- оформление проблемной ситуации (метод кейс-стади);
- сторителлинг* и т. д.

Как показывают результаты исследований [5–7, 16], один из эффективных приемов формирования интереса обучающихся к проблеме обеспечения

информационной безопасности — использование механизмов юмора в обучении, таких как «юмористическое изложение правил информационной безопасности, комиксы, карикатуры, шаржи, подбор курьезных случаев из практики, создание мемов, комиксов, подбор юмористических демотиваторов манипулятивным воздействиям в сети Интернет и др.» [17, с. 18].

На рисунке 3 представлен фрагмент комикса, разработанный в ходе реализации проекта с использованием сервиса Pixton, рассказывающий о доверчивости пользователей социальных сетей.

Сервис создания ментальных карт (карт знаний) — mindmup: <https://www.mindmup.com/>

Сервис позволяет быстро создавать карты знаний, добавлять изображения, ссылки на внешние интернет-ресурсы, прикреплять к отдельным узлам карты документы, кастомизировать внешний вид

* Сторителлинг (англ. storytelling — рассказывание историй) — неформальный метод обучения посредством повествования историй (мифов, сказок, притч, былин и пр.), которые являются выражением определенного принципа, ценности или идеологии. Истории более выразительны, увлекательны, интересны и легче ассоциируются с личным опытом, чем правила или директивы. Они лучше запоминаются, им придают больше значения, и их влияние на поведение людей оказывается сильнее [12].

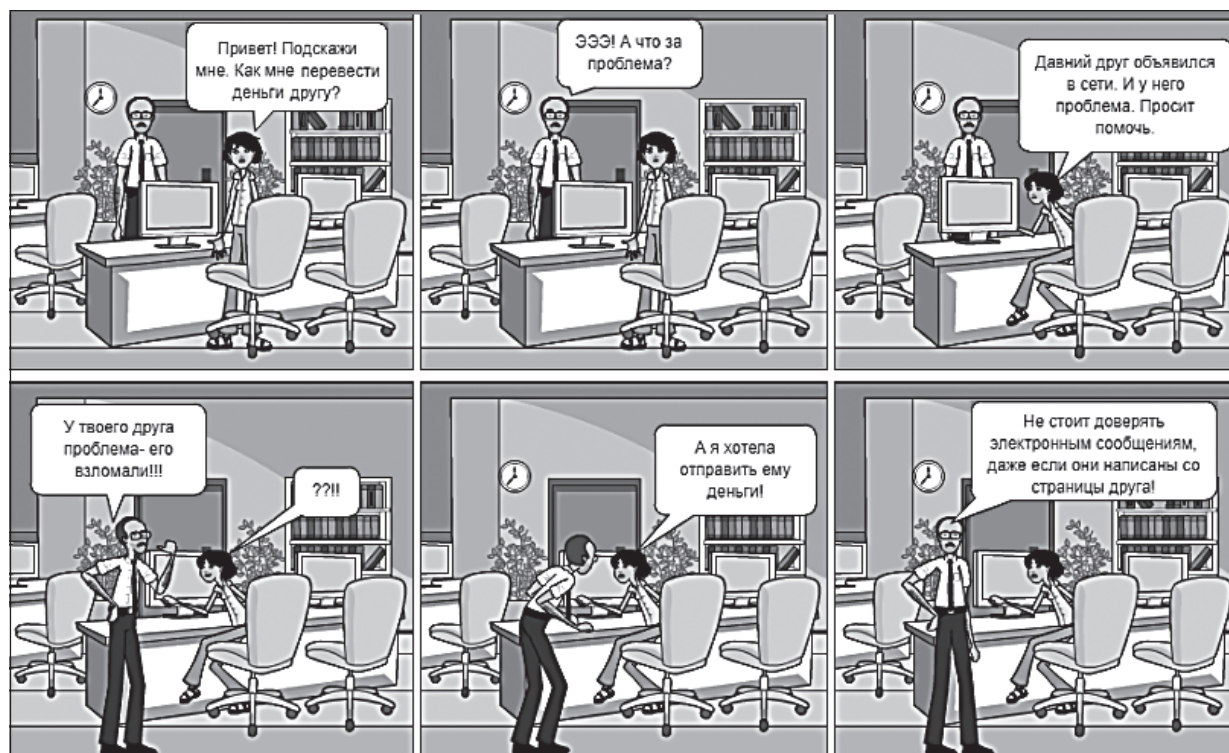


Рис. 3. Фрагмент комикса «Электронное вымогательство», созданного в сервисе Pixton

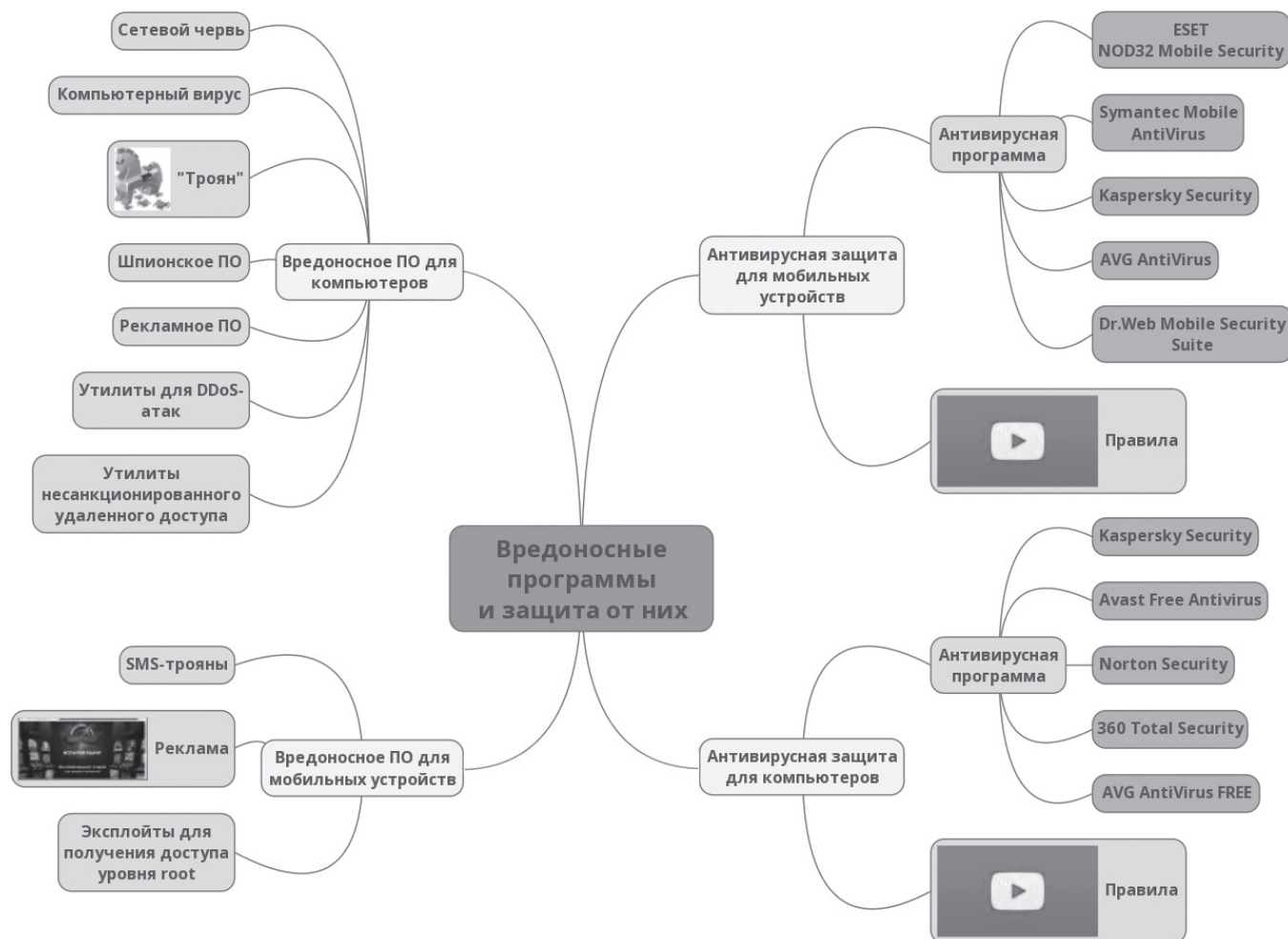


Рис. 4. Ментальная карта «Виды вредоносных программ и методы защиты от них» [15]

карты под требования пользователя. Созданные карты разрешается выгружать в форматах png, jpg, ppt, doc, pdf.

В качестве педагогических приемов использования ментальных карт можно выделить следующие:

- прием «ключевые понятия» — предлагается создать в онлайн-сервисе ментальные карты по изучаемым понятиям;
- прием «заполнение» — предлагается заполнить ментальную карту с пропущенными словами, используя онлайн-сервис, т. е. в данном случае студенты заполняют готовый шаблон ментальной карты;
- прием «пустая карта» — предлагается самостоятельно построить ментальную карту процесса, события, добавляя в нее мысли, идеи по учебной теме;
- прием «исправь ошибки» — в готовой ментальной карте предлагается найти допущенные ошибки;

- прием «оживи карту» — предлагается в готовую ментальную карту добавить интерактивные элементы (ссылки на внешние интернет-ресурсы с описанием базовых понятий ментальной карты; аудио-, видеофрагменты и др.);
- прием «установи соответствие» — предлагается нарисовать связи между элементами/ключевыми понятиями ментальной карты и др. [16, 19 и др.].

На рисунке 4 приведен пример ментальной карты по проекту «Виды вредоносных программ и методы защиты от них», в котором был реализован прием «оживи карту».

Сервис для создания инфографики — Piktochart: <https://piktochart.com>

Инфографика — один из наиболее популярных способов представления учебного материала, поскольку позволяет в наглядном виде представить большой объем информации. Однако стоит отметить, что разработка плаката с инфографикой требует не только



Рис. 5. Инфографика «Информационная безопасность в цифрах»

наличия знаний по учебной теме, но и творческого подхода, при этом процесс разработки достаточно трудоемок.

Педагогические возможности использования инфографики:

- реализация принципа наглядности;
- реализация интерактивности за счет использования интерактивных компонентов (ссылок, видео, аудио) для плакатов, хранящихся в электронном виде;
- развитие креативности, творческих способностей учащихся [2].

На рисунке 5 представлен пример использования сервиса Piktochart при разработке плаката с инфографикой «Информационная безопасность в цифрах».

Сервис хранения закладок — Symbaloo:
<https://www.symbaloo.com/>

Symbaloo — сервис для создания вебмиксов. Вебмикс (англ. webmix) — это компиляция (набор) плиток на определенную тему или по определенному предмету, каждая из которых — это ссылка на сервис или сайт. С помощью сервиса можно создать коллекцию ссылок по заданной теме, подготовить коллекцию полезных ссылок, сгруппировав их тематически, выделяя темы разным цветом, и поместить на стартовую страницу в браузер.

Педагогические возможности сервиса:

- создание коллекции ссылок на полезные интернет-ресурсы;
- совместное использование, редактирование коллекции ссылок;
- возможность распространения коллекции ссылок.

В качестве задания студентам, реализующим проект «Интернет: проблемы защиты интеллектуальной собственности», было предложено создать коллекцию

вебмиксов по отдельным темам. На рисунке 6 представлен фрагмент вебмикса, созданного в сервисе Symbaloo.

Сервис создания ленты времени — Sutori:
<https://www.sutori.com/>

Сервис позволяет оформлять в наглядном виде хронологию событий, включая аудио, видео, анимацию. Также имеется возможность реализовать опросы по ленте. В сервисе есть инструменты для контроля — создания тестовых заданий, контрольных вопросов. Подготовленную ленту времени можно встроить как объект embed на другие интернет-ресурсы.

Педагогические возможности ленты времени:

- наглядное представление истории отдельного учебного понятия;
- проведение контроля усвоения темы;
- совместное создание, редактирование и использование ленты времени.

На рисунке 7 представлена лента времени по истории развития компьютерных вирусов.

С декабря 2017 по апрель 2018 года нами был проведен опрос с целью оценки эффективности применения сетевых сервисов Веб 2.0 в рамках проектной деятельности. В опросе участвовали студенты бакалавриата, обучающиеся в Институте энергетики и автоматизированных систем и Институте гуманитарного образования ФГБОУ ВО «МГТУ им. Г. И. Носова» (в таблице представлены предложенные студентам вопросы и варианты ответов на них).

В опросе приняли участие 49 студентов педагогического образования. Были выявлены следующие показатели удовлетворенности реализацией проектной деятельности в сочетании с сервисами Веб 2.0: низкая — 8 %, средняя — 23 %, высокая — 69 %. Результаты анкетирования показали удовлетворенность студентов процессом обучения с использова-

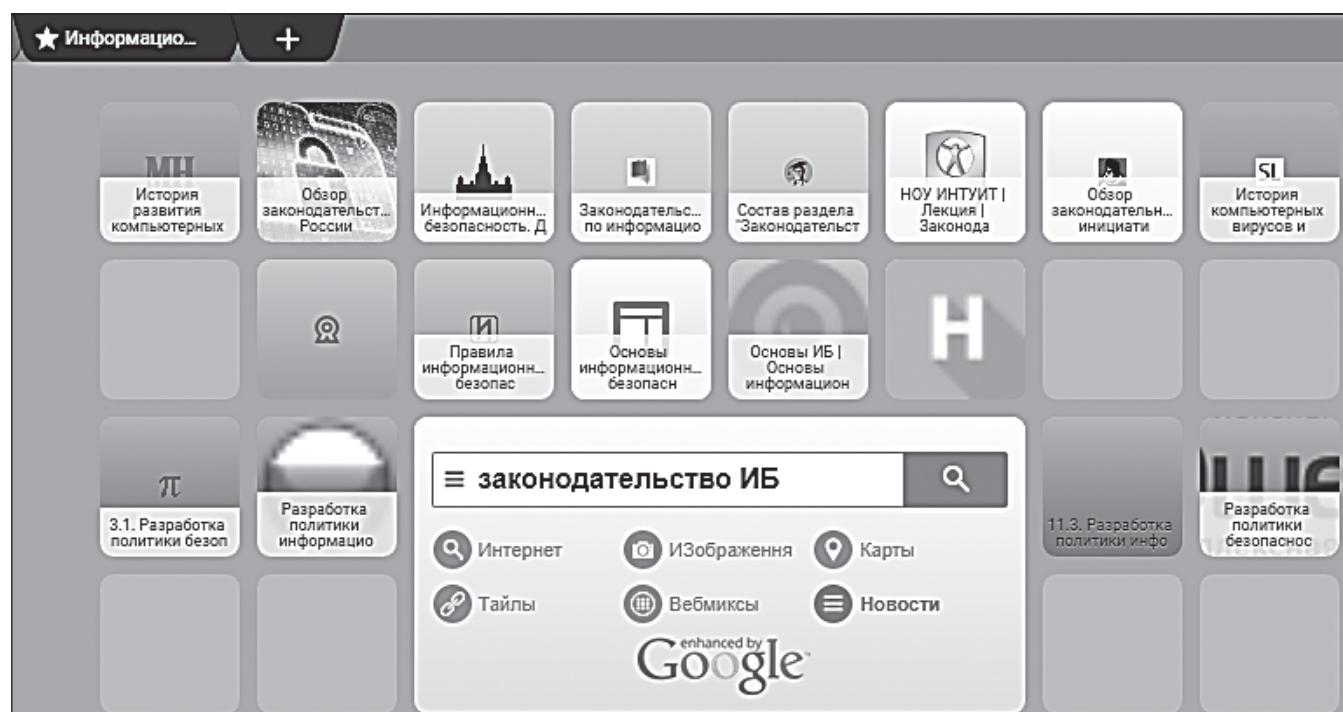


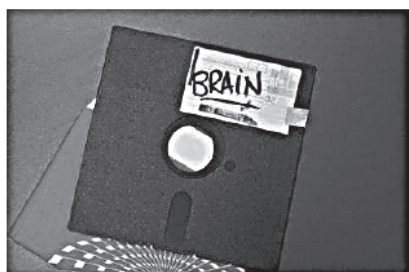
Рис. 6. Фрагмент вебмикса, созданного в сервисе Symbaloo

История развития компьютерных вирусов

Раньше вирусописательством занимались дети, студенты, школьники с целью самоутверждения, это было мелкое хулиганство. Сейчас - это бизнес!

1986 — Brain. Первый «вирус»-программа, проникающая в компьютер, заражающая все его файлы и стремящаяся распространиться на другие компьютеры.

1988 — Червь Морриса. Аспирант факультета вычислительной техники Корнелльского университета Роберт Т. Моррис решил собрать информацию обо всех пользователях компьютерной сети ARPANET.



1989 — AIDS. Джозеф Попп разослал в общей сложности 20 000 дискет с надписью: AIDS. Тех, кто запустил дискету, через 90 включений/выключений компьютера ждал сюрприз: программа шифровала и делала невидимыми все файлы, сообщая, что откроет доступ к ним только после того, как по определенному адресу в Панаме будет отправлен чек на \$189–378.

1998 — Back Orifice. Первый вирус, позволяющий злоумышленнику брать под контроль компьютер пострадавшего или даже целую сеть и управлять ею как системный администратор.



2000 — Love Letter. Человек получал от своего знакомого письмо с темой I Love You и вложенным файлом LOVE-LETTER-FOR-YOU.TXT. При открытии письмо заражало компьютер: вирус крал логины и пароли, уничтожал библиотеки текстов, музыки и изображений, а также рассылал сам себя всем контактам из адресной книги.



1988 — Jerusalem. Также известен как «пятница 13-е». Попадая в компьютер, ждал наступления ближайшей пятницы 13-го и тогда активировался, уничтожая любой файл, который пытался открыть пользователь.

1990 — Disk Killer. Английский компьютерный журнал PC Today решил осчастливить читателей, вложив в новый номер дискету с программами. Случайным «бонусом» к дискете оказался вирус DiskKiller: он прятался в каждом из 50 000 флоппи-дисков.

1992 — Peach. Первый вирус с функцией антиантивируса, начинавший жизнь на PC с удара по его защитной программе.

1995 — Concept. Первый вирус для Microsoft Word.



1997 — Bliss
Первый вирус для операционной системы Linux. В том же году вредоносное ПО научилось распространяться по электронной почте и FTP.

2004 — Sasser. Эпидемия этого червя привела к тому, что аэропорты из-за компьютерных сбоев отменяли рейсы, а отделения банков закрывались.

2007 — Storm. Приходил в систему в виде спама со вложенным файлом, при нажатии на который включал компьютер в сеть бот-нетов.

Рис. 7. Лента времени «История развития компьютерных вирусов»

Таблица

№ п/п	Вопросы	Варианты ответов
1	Применяете ли вы сетевые сервисы Веб 2.0 при реализации проектной деятельности?	• Да, всегда • Иногда применяю • Очень редко • Нет, не применяю
2	Зависит ли успех реализации проекта от выбора конкретного сетевого сервиса?	• Да • Нет • Все зависит от проекта
3	Считаете ли вы эффективным использование метода проектов в сочетании с информационно-коммуникационными технологиями в процессе обучения дисциплине «Информационная безопасность»?	• Да • Затрудняюсь ответить • Нет, было сложно • Нет, не вижу в этом положительного эффекта
4	Какие сетевые сервисы вы используете в проектах наиболее часто?	• Сервисы закладок • Сервисы ментальных карт • Сервисы инфографики • Сервисы лент времени • Сервисы презентаций • Сервисы управления проектом, совместных разработок • Сервисы комиксов • Сервисы опросов • Я не использую сервисы • Не знаю такие сервисы
5	Какую систему обучения вы предпочитаете?	• Объяснительно-иллюстративную • Проектную • Личностно-ориентированную • Эвристическую • Все зависит от предмета • Не могу выбрать, не знаю их особенностей
6	Смогли ли вы достигнуть поставленных целей при реализации проекта?	• Да, цель полностью была достигнута • Да, но не полностью • Нет, цель не была достигнута • Нет, у меня не получилось выполнить проект
7	Хотели бы вы еще принять участие в проектах с использованием сетевых сервисов Веб 2.0?	• Да • Нет • Пока не определился(лась)

нием метода проектов, а также активное использование при реализации проектов сервисов Веб 2.0, предназначенных для создания ментальных карт, инфографики, лент времени.

Современные сетевые сервисы предоставляют широкие возможности для педагогов как учебные инструменты, повышающие эффективность обучения. Использование сетевых сервисов Веб 2.0 при реализации проектного подхода в процессе обучения информационной безопасности позволяет:

- повышать интерес студентов к изучению и соблюдению правил информационной безопасности;
- активизировать информационный обмен, коммуникацию среди студентов;
- развивать способности обучающихся к кооперации, сотрудничеству, коллективной работе и конструктивному взаимодействию;
- формировать собственный уникальный цифровой контент по вопросам информационной безопасности и др.

В данной статье описаны лишь несколько сервисов, однако стоит отметить, что в проектной деятельности можно использовать и другие возможности, такие как:

- создание мультфильмов (Powtoon);
- создание мемов (risovach);
- разработка и размещение презентаций (emazi);
- создание текстовых квестов (kvester);
- разработка дидактических игр (umaigra);
- проведение опросов (GoogleForms);
- генерирование облака слов (wordart);
- создание сайтов, блогов (wix) и т. д.

Список использованных источников

1. Государственная программа «Информационное общество» (2011–2020 годы). http://www.consultant.ru/document/cons_doc_LAW_162184/4b6b1ec3d9a61a8204d8fdc520469db8e0daa367/
2. Карманова Е. В., Голощапов А. С., Файзулин Е. Б. Использование сервисов Веб 2.0 в поддержку дистанционного обучения // Сборник материалов и докладов IV Всероссийской научно-практической конференции «Коммуникативные и образовательные возможности современных технологий» (г. Екатеринбург, 6 июня 2016 года). Екатеринбург: ИОЦ «Информед», 2016.

3. Курзаева Л. В., Чусавитина Г. Н. К вопросу о формировании требований к компетенциям личности в области информационной безопасности в системе высшего профессионального образования // *Фундаментальные исследования*. 2013. № 8-5.

4. Мовчан И. Н., Чернова Е. В., Чусавитина Г. Н. Учебный проект как одна из форм противодействия киберэкстремизму среди школьников // *Фундаментальные исследования*. 2015. № 9-3.

5. Мусийчук М. В. Развитие креативности, или Дюжина приемов остроумия. М.: Флинта, 2013.

6. Мусийчук М. В., Мусийчук С. В. Юмор в образовании как эффективный способ превратить «Ха-Ха» в «Ага!» // *Академический журнал Западной Сибири*. 2014. № 3 (52). Т. 10.

7. Мусийчук М. В., Мусийчук С. В., Макарова А. К. Когнитивно-аффективные основания юмора как эффективное средство формирования мировоззрения в процессе образования // *Концепт*. 2015. Т. 3.

8. Пахомова Н. Ю. Метод учебного проекта в образовательном учреждении: пособие для учителей и студентов педагогических вузов. 3-е изд., испр. и доп. М.: АРКТИ, 2005.

9. Полат Е. С., Бухаркина М. Ю., Моисеева М. В., Петров А. Е. Новые педагогические и информационные технологии в системе образования: учебное пособие / под ред. Е. С. Полат. 4-е изд., стереотип. М.: Академия, 2009.

10. Программа «Цифровая экономика Российской Федерации» (Распоряжение Правительства Российской Федерации от 28 июля 2017 года № 1632-п). <http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPg u4bvR7M0.pdf>

11. Сторителлинг. <http://www.trainings.ru/library/dictionary/storytelling/>

12. Чернова Е. В. Информационная безопасность для гуманитариев: учебное пособие. Магнитогорск: МГТУ им. Г. И. Носова, 2016.

13. Чусавитин М. О., Чусавитина Г. Н., Курзаева Л. В. Разработка модели компетентности будущих учителей информатики и ИКТ в области обеспечения информационной безопасности // *Фундаментальные исследования*. 2013. № 10-13.

14. Чусавитина Г. Н. Проблемы организации учебно-воспитательной работы со школьниками в целях нейтрализации негативного воздействия ИКТ // *Вестник Московского государственного областного университета. Серия «Открытое образование»*. 2006. Т. 1. № 2.

15. Чусавитина Г. Н. Развитие компетенций научно-педагогических кадров по обеспечению информационной безопасности в ИКТ-насыщенной среде // *Спрос и пред-*

ложение на рынке труда и рынке образовательных услуг в регионах России. Сборник докладов по материалам Восьмой Всероссийской научно-практической Интернет-конференции (27–28 октября 2011 года). Кн. I. Петрозаводск: Изд-во ПетрГУ, 2011.

16. Чусавитина Г. Н. Формирование компетенций в области обеспечения информационной безопасности у студентов педагогических направлений вуза // *Информатика и образование*. 2018. № 1.

17. Чусавитина Г. Н., Курзаева Л. В., Давлеткиреева Л. З., Чусавитин М. О. Подготовка будущих учителей к обеспечению информационной безопасности: монография. Магнитогорск: МГТУ им. Г. И. Носова, 2017. <http://catalog.inforeg.ru/Inet/GetEzineByID/315315>

18. Чусавитина Г. Н., Масленникова О. Е., Давлеткиреева Л. З. Подготовка будущих ИТ-специалистов в области обеспечения интероперабельности электронной науки и образования // *Разработка инновационных механизмов повышения конкурентоспособности выпускников ИТ-специальностей вуза в условиях монопромышленного города (сборник статей)* / под ред. Г. Н. Чусавитиной, Л. З. Давлеткиреевой. Магнитогорск: МаГУ, 2012.

19. Чусавитина Г. Н., Мусийчук М. В. Педагогические аспекты проблемы противодействия угрозам в сети Интернет // *Интернет-журнал «Мир науки»*. 2017. Т. 5. № 6. <https://mir-nauki.com/PDF/68PDMN617.pdf>

20. Шарипов Ф. В. Технология проектного обучения: учебное пособие. Уфа: Республиканский УНМЦ МО Республики Башкортостан, 2010.

21. Chernova E. V. Teachers training for prevention of pupils deviant behavior in ICT // *Conference on Information Technologies in Science, Management, Social Sphere and Medicine (ITSMSM-2016)*. Conference proceedings. Atlantis Press, 2016.

22. Chusavitina G., Zerkina N. Cyber extremism preventive measures in training of future teachers // *International multidisciplinary scientific conference on social sciences and arts SGEM*. 2015. Vol. 2.

23. Chusavitina G., Zerkina N. Informational ethics teaching for future information technology specialist // *International multidisciplinary scientific conference on social sciences and arts SGEM*. 2015. Vol. 2.

24. Kurzaeva L. V. Future teachers' competence forming in the sphere of information security: modern requirements & means // *Conference on Information Technologies in Science, Management, Social Sphere and Medicine (ITSMSM-2016)*. Conference proceedings. Atlantis Press, 2016.

25. Zerkina N. N., Lomakina E. A., Chusavitina G. N. Verbal aggression in virtual environment // *Modern Journal of Language Teaching Methods*. 2017. Т. 7. No. 8.1.

НОВОСТИ

Приложение выборбудущего.рф признано лучшим среди всех проектов органов исполнительной власти РФ

Мультимедийное приложение выборбудущего.рф признано лучшим среди всех проектов органов исполнительной власти РФ, сообщает Федеральная служба по надзору в сфере образования и науки. Приложение разработано Рособрнадзором и рассказывает о различных процедурах оценки качества образования.

«Вместе с героем приложения мальчиком Алексеем пользователи могут в доступной и понятной форме познакомиться с такими процедурами оценки качества образования как: Национальные исследования качества образования

(НИКО), Всероссийские проверочные работы (ВПР), итоговая аттестация в девятих классах (ГИА-9) и Единый государственный экзамен (ЕГЭ)», — говорится в сообщении.

Приложение регулярно обновляется. Недавно в него были добавлены актуальные плакаты, разъясняющие, с какой информацией следует ознакомиться абитуриентам и их родителям при выборе вуза, а также как поступать при приостановлении действия или лишении вуза аккредитации или лицензии на осуществление образовательной деятельности.

(По материалам федерального портала «Российское образование»)