**Г. Н. Чусавитина,**

***победитель конкурса ИНФО-2017 в номинации «Правила информационной безопасности — изучаем и соблюдаем», Магнитогорский государственный технический университет им. Г. И. Носова, Челябинская область***

# ФОРМИРОВАНИЕ КОМПЕТЕНЦИЙ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ У СТУДЕНТОВ ПЕДАГОГИЧЕСКИХ НАПРАВЛЕНИЙ ВУЗА

***Аннотация***

В статье описывается опыт подготовки будущих учителей к обеспечению информационной безопасности в системе образования. Обосновывается необходимость подготовки педагогов, компетентных в сфере формирования культуры информационной безопасности у подрастающего поколения и обеспечения защиты информационной инфраструктуры образовательного учреждения. Раскрыто содержание учебной дисциплины «Информационная безопасность», представлена методика формирования компетенций у будущего учителя в сфере обеспечения информационной безопасности. Приводятся примеры применения активных методов обучения информационной безопасности будущих бакалавров педагогического образования.

***Ключевые слова:*** информационная безопасность, информационная безопасность в образовании, подготовка педагогов, компетентность в сфере обеспечения информационной безопасности, активные методы обучения, агрессивная информационная среда, деструктивный информационный контент.

В условиях цифрового общества применение информационно-коммуникационных технологий наряду с положительным влиянием оказывает и отрицательное, связанное с нарушениями информационной безопасности, с угрозами деструктивных информационных воздействий по отношению к индивидууму, социальной группе, государству и человечеству в целом.

В последние годы во всем мире отмечается рост компьютерных преступлений. По оценкам экспертов Исследовательского центра CSIS (Center for Strategic and International Studies), ущерб глобальной экономике от различных видов киберпреступлений составляет примерно $400 млрд. в год. Активизируются религиозные, националистические и иные деструктивные, в том числе экстремистские, движения, которые посредством сетевого взаимодействия (социальных сетей, видеохостингов, форумов, блогов, электронной почты и т. д.) вовлекают в свою деятельность молодых людей.

Как показывают проводимые исследования, именно молодежь наиболее подвержена деструктивному влиянию в сети Интернет [10, 13–15, 20–22 и др.]. Во всем мире увеличивается количество обращений молодежи к нежелательному контенту (рис. 1), около 80 % участников организаций экстремистского характера составляют лица, возраст которых не превышает 30 лет, в том числе несовершеннолетние лица 14–18 лет.

К негативным явлениям в цифровом обществе исследователи относят [13, 15, 16 и др.]:

- информационные перегрузки;
- энтропию;
- агрессивное массово-коммуникативное воздействие (пропаганду ненависти и насилия,

***Контактная информация***

**Чусавитина Галина Николаевна**, канд. пед. наук, профессор, профессор 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:* Gala_m27@mail.ru

**G. N. Chusavitina,**
Nosov Magnitogorsk State Technical University, Chelyabinsk Region

## FORMING COMPETENCIES IN THE FIELD OF ENSURING INFORMATION SECURITY FOR STUDENTS OF PEDAGOGICAL DIRECTIONS OF UNIVERSITIES

***Abstract***

The article describes the experience of training future teachers for ensuring information security in the education system. The necessity of training teachers competent in the sphere of formation of information security culture for the younger generation and ensuring the protection of the information infrastructure of the educational institution is substantiated. The content of the educational discipline "Information Security" is considered, the methodology of forming competencies for the future teacher in the field of information security is given. Examples of the use of active methods of training in the field of information security for future bachelors of pedagogical education are given.

***Keywords:*** information security, information security in education, training of teachers, competence in the field of information security, active teaching methods, aggressive information environment, destructive information content.


*Рис. 1. Статистика запросов подростков в сети Интернет*

дезинформацию, манипуляцию сознанием, распространение слухов и др.);

- ресоциализацию (подмену реального бытия в человеческом обществе виртуальным бытием в сети Интернет);
- виртуализацию (игнорирование или виртуализацию ответственности);
- провокационизм и инициацию конфликтных ситуаций;
- примитивизацию (упрощение форм, способов коммуникации);
- вульгаризацию (популяризацию нецензурных выражений, порнографии в интернет-контенте);
- криминализацию;
- игроизацию (процесс проникновения различных элементов игрового мира в другие сферы бытия) и пр.

В сети пользователи могут подвергаться различным интернет-угрозам. В таблице 1 приведены результаты проведенного нами исследования среди студентов первого-второго курсов бакалавриата, обучающихся в Институте энергетики и автоматизированных систем и Институте гуманитарного образования ФГБОУ ВО «МГТУ им. Г. И. Носова» [16].

Деструктивное воздействие информационных ресурсов интернета может проявляться в нарушениях физического и психического здоровья пользователей, в нанесении ущерба в личной, социальной, экономической, политической сферах. Молодежь является мишенью негативных информационно-психологических воздействий в интернете, она наиболее склонна к аддиктивному, асоциальному и делинквентному поведению в ИКТ-насыщенной среде, является особо уязвимой для идей «цветных» и «твиттерных» рево-

*Таблица 1*

**Результаты анкетирования бакалавров первого-второго курсов (май 2017 года)**

| № п/п | Вопрос | Варианты ответов | Результаты анкетирования | | | |
|---|---|---|---|---|---|---|
| | | | 1-й курс (33 чел.) | | 2-й курс (34 чел.) | |
| | | | % | Кол-во | % | Кол-во |
| 1 | Подвергались ли вы негативным воздействиям в интернете? | Подвергался оскорблениям | 42,42 | 14 | 38,25 | 13 |
| | | Подвергался кибербуллингу* | 39,39 | 13 | 44,11 | 15 |
| | | Подвергался троллингу** | 18,19 | 6 | 17,64 | 6 |
| | | Ничему не подвергался | 0 | 0 | 0 | 0 |
| 2 | В какой из сетевых сред вы встречались с этими действиями? | Социальные сети | 63,63 | 21 | 64,8 | 22 |
| | | Раздел комментариев на веб-сайте | 6,07 | 2 | 2,94 | 1 |
| | | Онлайн-игры | 24,24 | 8 | 29,41 | 10 |
| | | Форумы | 6,06 | 2 | 2,94 | 1 |
| 3 | Выберите три вида угроз, которые, на ваш взгляд, наиболее часто встречаются в интернете? | Языковая агрессия | 12,12 | 4 | 14,7 | 7 |
| | | Информационное манипулирование | 9,09 | 3 | 11,76 | 4 |
| | | Спам | 15,15 | 5 | 11,76 | 4 |
| | | Кибермошенничество | 12,12 | 4 | 14,7 | 5 |
| | | Вредоносные программы | 15,15 | 5 | 17,6 | 6 |
| | | Кибербуллинг | 12,12 | 4 | 2,94 | 1 |
| | | Нежелательный контент | 18,19 | 6 | 5,88 | 2 |
| | | Кибертерроризм | 6,06 | 2 | 14,7 | 5 |

* Кибербуллинг (от *англ.* cyber-bullying), или интернет-травля — преднамеренные и продолжающиеся на протяжении определенного периода времени агрессивные действия с целью нанесения психологического вреда человеку, которые осуществляются через электронную почту, сервисы мгновенных сообщений, в чатах, социальных сетях, на веб-сайтах, а также посредством мобильной связи.

** Троллинг (от *англ.* trolling — ловля на блесну) — размещение на различных интернет-ресурсах провокационных статей либо сообщений с целью развития конфликта между пользователями с сопровождением взаимных оскорблений и т. п. Главной целью троллинга является привлечение других пользователей к дискуссии путем саркастического, провокационного, подстрекательского или юмористического содержания сообщений тролля.

люций, насильственного экстремизма, ксенофобии, нетерпимости и террористической радикализации. Интернет-зависимость порождает и всевозможные экономические проблемы: огромные потери от пиратской продукции несут правообладатели, наносится ущерб компаниям от пользования работников соцсетями в рабочее время, интернет-пользователи тратят огромные деньги на необоснованные онлайн-покупки и пр.

Большая роль в педагогической диагностике, профилактике и коррекции негативных информационных воздействий на детей и молодежь в интернете отводится педагогам. *Среди первоочередных задач цифрового общества — не только совершенствование системы подготовки кадров в сфере защиты информации, но и формирование компетентности в области информационной безопасности у выпускников вузов педагогических направлений* [3, 9, 18–22 и др.].

Констатируя разработку отдельных аспектов обозначенной проблемы, мы пришли к выводу о том, что в системе высшего образования существует проблема, связанная с необходимостью обобщения, систематизации исследований, разработки комплекса теоретико-методологических оснований и методического обеспечения построения концепции и педагогической модели формирования у студентов компетенции в сфере обеспечения информационной безопасности (ОИБ). При этом *под* ***компетенцией будущего учителя в области обеспечения информационной безопасности*** *мы понимаем интегрированную характеристику качеств личности, позволяющую осуществлять профессиональную и социальную деятельность с учетом требований к информационной безопасности, определяемую совокупностью ценностей личности и ее мотивов к саморазвитию в области информационной безопасности, знаниями основ информационной безопасности, умениями, навыками и опытом успешной защиты информационной инфраструктуры образовательного учреждения (профессионально значимой информации), а также эмоционально-волевой устойчивостью и способностью противостоять угрозам информационной безопасности* [3, 11, 15 и др.].

В ходе проведенного исследования путей совершенствования системы подготовки будущих учителей информатики к обеспечению информационной безопасности в учебно-воспитательном процессе вуза [3, 9, 10, 13, 16 и др.] нами была разработана **методика формирования у студентов компетенции в сфере обеспечения информационной безопасности**. Обобщенная модель методики формирования компетенции в области ОИБ представлена в таблице 2 [11, 12].

Проблемы обеспечения информационной безопасности рассматриваются в различных дисциплинах учебного плана подготовки бакалавров по направлению «Педагогическое образование» («Право», «Основы безопасности жизнедеятельности» и др.). Однако уровень формируемых в данных дисциплинах компетенций в области ОИБ явно недостаточен в условиях развивающегося информационного общества. Мы считаем возможным *реализацию разработанной методики в рамках преподавания дисциплины «Информационная безопасность», которую необходимо включить во все учебные планы подготовки будущих учителей*.

***Целью изучения дисциплины «Информационная безопасность»*** является обучение студентов — будущих учителей принципам и средствам обеспечения информационной безопасности личности школьников, конкретных образовательных объектов и учреждений, общества и государства в целом.

В таблице 3 представлены основные разделы дисциплины «Информационная безопасность» и приведено их краткое содержание.

С целью решения проблем активизации учебно-познавательной деятельности студентов, обучающихся в Институте энергетики и автоматизированных систем и Институте гуманитарного образования ФГБОУ ВО «МГТУ им. Г. И. Носова», в процессе обучения информационной безопасности и защите информации нами использовались разнообразные

*Таблица 2*

**Модель методики формирования компетенции в области обеспечения информационной безопасности**

<table>
<tr><th colspan="2">НОРМАТИВНО-ЦЕЛЕВОЙ БЛОК</th></tr>
<tr><td>Социальный заказ общества и государства:<br>подготовка учителей информатики, обладающих компетенцией в области обеспечения информационной безопасности (ОИБ)</td><td>Требования ФГОС ВО<br>по направлению 440000 «Образование и педагогические науки» к уровню подготовки в области информационной безопасности и защиты информации</td></tr>
<tr><td colspan="2">Цель:<br>формирование у будущих учителей информатики компетенции в области обеспечения информационной безопасности в процессе профессиональной подготовки</td></tr>
<tr><th colspan="2">МЕТОДОЛОГИЧЕСКИЙ БЛОК</th></tr>
<tr><td>Подходы:<br>• ценностный;<br>• компетентностный;<br>• личностно-деятельностный</td><td>Принципы:<br>• формирования ценностных ориентаций;<br>• развивающего и воспитывающего характера обучения;<br>• личностно-ориентированного образования;<br>• самостоятельности, формирования опыта решения проблем;<br>• самоактуализации и развития индивидуальности студентов;<br>• деятельности;<br>• непрерывности;<br>• целостности;<br>• сознательности и активности обучающихся</td></tr>
</table>

*Окончание табл. 2*

<table>
<tr><td colspan="5">СОДЕРЖАТЕЛЬНО-ОРГАНИЗАЦИОННЫЙ БЛОК</td></tr>
<tr><td colspan="5">Содержание обобщенной специальной компетенции<br>«способен обеспечить информационную безопасность (ИБ) и защиту информации (ЗИ) в ключевых сферах будущей профессиональной деятельности»:<br>• способен разрабатывать и реализовывать учебные модули программ базовых и элективных курсов по проблемам ИБ на различных образовательных ступенях в различных ОУ;<br>• способен формировать и использовать безопасную электронную информационно-образовательную среду (ЭИОС);<br>• способен проводить научные исследования по гуманитарной составляющей проблемы ИБ и применять результаты научных исследований при решении конкретных образовательных задач;<br>• готов исследовать, проектировать, организовывать и оценивать реализацию управленческого процесса с использованием ЭИОС;<br>• готов к осуществлению педагогического проектирования ЭИОС, образовательных программ и индивидуальных образовательных маршрутов по проблемам ИБ и защиты информации (ЗИ);<br>• готов к разработке и реализации методик обучения ИБ и обеспечения безопасности ЭИОС;<br>• способен изучать и формировать культурные потребности и повышать культурно-образовательный уровень различных групп населения по вопросам ИБ</td></tr>
<tr><td colspan="5">Компоненты компетенции</td></tr>
<tr><td>Мотивационный компонент</td><td>Когнитивный компонент</td><td>Поведенческий компонент</td><td>Ценностно-смысловой компонент</td><td>Эмоционально-волевой компонент</td></tr>
<tr><td colspan="5">Жизненный цикл компетенции (этапы)</td></tr>
<tr><td colspan="2">Этап формирования</td><td colspan="2">Этап совершенствования</td><td>Этап применения</td></tr>
<tr><td colspan="5">Организационно-педагогические условия формирования компетенции:<br>• обеспечение направленности содержания учебного и воспитательного процесса на противодействие деструктивным явлениям в киберпространстве на всех этапах подготовки учителя информатики;<br>• становление (формирование) субъектной позиции будущих учителей информатики в области ОИБ путем включения их в регулярную проектную и рефлексивную деятельность на занятиях в вузе;<br>• формирование у студентов опыта защиты информационной инфраструктуры образовательного учреждения от угроз информационных воздействий посредством разработки и реализации спецкурса «Информационная безопасностьв системе открытого образования»</td></tr>
<tr><td colspan="5">Методическое обеспечение формирования компетенции:</td></tr>
<tr><td colspan="2">Формы:<br>• лекции;<br>• лабораторные работы;<br>• практические занятия;<br>• деловые игры;<br>• учебные конференции;<br>• учебные и профессиональные практики;<br>• научно-исследовательская работа и др.</td><td colspan="2">Методы:<br>• метод проектов;<br>• игровые методы;<br>• моделирование;<br>• исследовательские методы;<br>• методы изучения ситуаций и опыта практической деятельности;<br>• мозговой штурм и др.</td><td>Средства:<br>• печатные;<br>• аудиовизуальные;<br>• наглядные;<br>• мультимедийные ресурсы;<br>• интернет-ресурсы;<br>• программно-аппаратные комплексы и др.</td></tr>
<tr><td colspan="5">ОЦЕНОЧНО-РЕЗУЛЬТАТИВНЫЙ БЛОК</td></tr>
<tr><td colspan="5">Критерии сформированности компетенции</td></tr>
<tr><td>Мотивационный</td><td>Когнитивный</td><td>Поведенческий</td><td>Ценностно-смысловой</td><td>Эмоционально-волевой</td></tr>
<tr><td colspan="5">Уровни сформированности компетенции</td></tr>
<tr><td colspan="2">Пороговый</td><td colspan="2">Базовый</td><td>Продвинутый</td></tr>
<tr><td colspan="5">РЕЗУЛЬТАТ</td></tr>
<tr><td colspan="5">Переход будущего учителя информатики на более высокий уровень сформированности компетенции в области обеспечения информационной безопасности</td></tr>
</table>

активные методы обучения, такие как ментальные карты, кейс-метод, метод проектов и др. (см. табл. 2, «Методическое обеспечение формирования компетенции») [1, 2, 4, 5, 7, 22 и др.].

Так, **применение ментальных карт в обучении информационной безопасности** позволяет преподавателям разнообразить и упростить учебный процесс, повысить мотивацию к запоминанию большого количества учебного материала, служит для облегчения восприятия сложных многоуровневых процессов [1]. Нами были использованы различные приемы применения ментальных карт (см. *Приложение А «Приемы использования ментальных карт»*), причем построение их осуществлялось студентами как вручную, так и с использованием различных сервисов для создания ментальных карт. В *Приложении Б* представлен анализ основных сервисов, используемых для создания ментальных карт.

*Таблица 3*

**Содержание дисциплины «Информационная безопасность» для студентов бакалавриата по направлению «Педагогическое образование»**

| № п/п | Основные разделы дисциплины | Содержание раздела |
|---|---|---|
| 1 | Основы информационной безопасности и защиты информации | 1.1. Актуальность проблемы обеспечения безопасности в цифровом обществе.<br>1.2. Основные понятия и определения информационной безопасности.<br>1.3. Основные составляющие информационной безопасности.<br>1.4. Наиболее распространенные угрозы информационной безопасности.<br>1.5. Виды мер обеспечения информационной безопасности |
| 2 | Законодательный и нормативно-правовой уровни обеспечения информационной безопасности | 2.1. Обзор российского законодательства в области информационной безопасности.<br>2.2. Стандарты и спецификации в области информационной безопасности.<br>2.3. Морально-этические нормы поведения в цифровом мире.<br>2.4. Организационно-правовые механизмы обеспечения информационной безопасности в образовательных учреждениях |
| 3 | Административный и процедурный уровни обеспечения информационной безопасности | 3.1. Анализ рисков информационной безопасности.<br>3.2. Политика информационной безопасности.<br>3.3. Программа работ в области обеспечения информационной безопасности.<br>3.4. Основные классы мер процедурного уровня:<br>• управление персоналом;<br>• физическая защита;<br>• поддержание работоспособности;<br>• реагирование на нарушения режима безопасности;<br>• планирование восстановительных работ |
| 4 | Основные программно-технические меры обеспечения информационной безопасности | 4.1. Основные понятия программно-технического уровня информационной безопасности.<br>4.2. Особенности современных информационных систем, существенные с точки зрения безопасности.<br>4.3. Идентификация и аутентификация, управление доступом.<br>4.4. Шифрование, контроль целостности.<br>4.5. Анализ защищенности. Обеспечение высокой доступности |
| 5 | Информационная безопасность в образовании | 5.1. Основные риски и угрозы информационной безопасности образовательного учреждения.<br>5.2. Безопасное использование интернета в образовательном учреждении.<br>5.3. Антивирусная защита информационных ресурсов образовательного учреждения.<br>5.4. Контентная фильтрация.<br>5.5. Защита персональных данных.<br>5.6. Безопасность учащихся при использовании информационных технологий:<br>• профилактика и противодействие идеологии киберэкстремизма среди молодежи;<br>• деструктивные группы в интернете;<br>• коррекция девиантного (аддиктивного, делинквентного) поведения школьников в сфере ИКТ и др. |

В процессе обучения использовались различные виды индивидуальной и групповой деятельности студентов по построению и использованию ментальных карт (разработка коллективных интеллект-карт), а также творческие домашние задания по созданию ментальных карт процессов или событий, мыслей или идей по вопросам (темам) курса. Основные способы применения ментальных карт при организации различных видов занятий со студентами по дисциплине «Информационная безопасность» приведены в таблице 4.

Интеллектуальные карты эффективно применялись при организации исследовательской и проектной деятельности студентов как на аудиторных занятиях, так и во внеаудиторной деятельности.

С примерами ментальных карт, разработанных студентами в ходе изучения дисциплины «Информационная безопасность», можно познакомиться в *Приложении В*.

Другим активным методом, который используется нами при подготовке будущих учителей в области информационной безопасности, является **кейс-метод (метод анализа конкретных ситуаций)**. Кейс-метод основывается на применении в образовательном процессе специально смоделированной ситуации в целях анализа, выявления проблем, поиска альтернативных решений и принятия оптимального из них [2 и др.]. Данный метод позволяет студентам получить не только теоретические, но и практические знания.

В процессе преподавания нами использовались не только текстовые (печатные) кейсы, но и мультимедийные и видеокейсы. Кейсы применялись не только для обучения, но и для текущего и итогового контроля по дисциплине (рис. 2).

Методика применения кейса в образовательном процессе включает в себя:

- знакомство студентов с темой кейса;
- рассмотрение проблемной ситуации кейса;
- решение кейса;
- оценку кейса;
- прохождение теста на основе приобретенных знаний во время выполнения кейса;
- подведение итогов.

*Таблица 4*

**Формы занятий и приемы применения ментальных карт**

| Форма занятия | Прием применения ментальных карт | Описание приема |
|---|---|---|
| Лекция | Прием «Заполнение» | При конспектировании лекционного материала обучающиеся заполняют готовый шаблон ментальной карты |
| | Прием «Ключевые понятия» | При конспектировании лекции студенты достраивают ментальную карту, отражающую ключевые понятия темы |
| Лабораторная работа | Прием «Ключевые понятия» | В компьютерной аудитории бакалаврам предлагается создать в онлайн-сервисе в готовых шаблонах ментальные карты по изучаемым ключевым понятиям |
| | Прием «Заполнение» | В компьютерной аудитории студентам предлагается заполнить ментальную карту с пропущенными словами, используя онлайн-сервис |
| | Прием «Пустая карта» | Обучающимся предлагается самим построить ментальную карту процесса, события, внеся в нее мысли или идеи по теме занятия |
| Самостоятельная работа | Прием «Ключевые понятия» | В рамках самостоятельной работы бакалавры строят ментальные карты по основным понятиям |
| | Прием «Оживи карту» | Обучающимся предлагается создать ментальную карту, используя как можно больше ассоциативных связей (изображений, видеофрагментов, цветовых решений и пр.), чтобы придать карте большую эмоциональную выразительность |
| | Прием «Заполнение» | Студенты заполняют ментальные карты, в которых пропущены ключевые моменты |
| | Прием «Дополнение» | Обучающимся предлагается дополнить имеющуюся ментальную карту |
| | Прием «Пустая карта» | Студентам предлагается самим построить ментальную карту по определенной теме |
| | Прием «Установи соответствие» | Обучающимся предлагается правильно установить соответствие между понятиями, отраженными в ментальной карте |
| | Прием «Исправь ошибки» | Студентам предлагается исправить ошибки в имеющейся ментальной карте |
| | Прием «Что хотел сказать автор?» | Обучающимся предлагается, используя готовую ментальную карту, описать представленный на ней процесс, событие, идею или мысль автора |

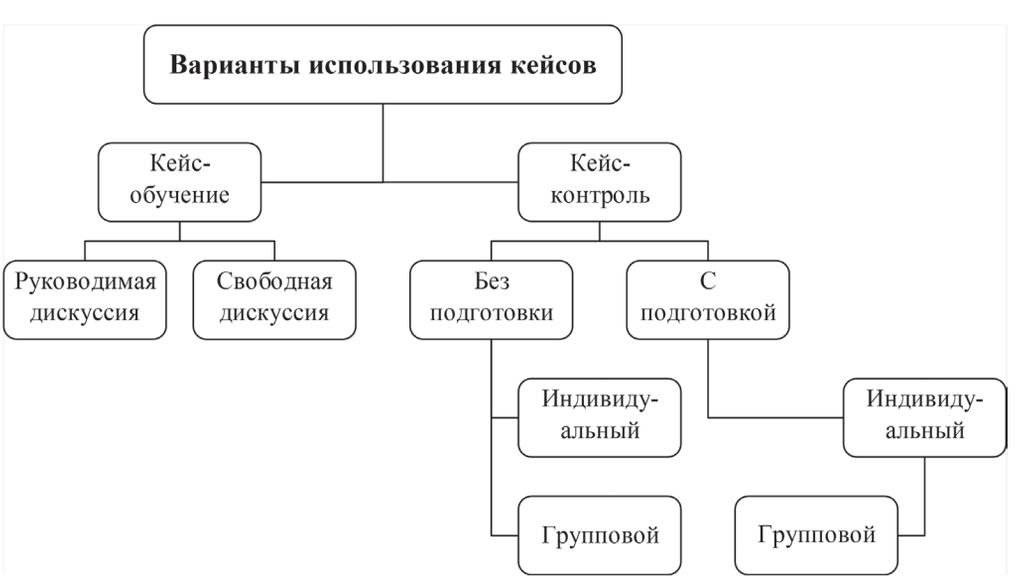


*Рис. 2. Варианты использования кейсов*

Нами разработаны кейсы по темам: «Деструктивные группы в социальных сетях — угроза обществу», «Способы противодействия манипуляциям в сети Интернет: критичность мышления; бесстрашие и уверенность в себе и др.», «Кибербуллинг — меры борьбы», «Профилактика киберэкстремизма среди молодежи» и др. Студенты принимали участие в разработке пакета кейсов по теме «Виды манипуляций в сети Интернет» (использование стереотипов, «наклеивание ярлыков», повторение информации, утверждение, постановка риторических вопросов, полуправда, «спираль умолчания», анонимный авторитет, «обыденный рассказ» и др.; технологии манипуляций в сети Интернет: спам и троллинг).

Одним из действенных приемов пробуждения дополнительного интереса студентов к проблеме обеспечения информационной безопасности является использование игровых методик и механизмов юмора в обучении, который справедливо признается одной из важнейших составляющих процесса обучения и творческой деятельности [5, 6, 8 и др.]. Например, юмористическое изложение правил информационной безопасности, комиксы, карикатуры, шаржи, подбор курьезных случаев из практики, создание мемов, подбор юмористических демотиваторов манипулятивным воздействиям в сети Интернет и др.

При подготовке будущих учителей в области информационной безопасности в образовательном процессе использовался **метод проектов** [4 и др.]. Виды проектов, реализуемых в дисциплине «Информационная безопасность», представлены в таблице 5.

С целью противодействия распространению идей киберэкстремизма среди молодежи и предотвращения вовлечения ее в киберэкстремистскую деятельность силами преподавателей и студентов Института энергетики и автоматизированных систем ФГБОУ ВО «МГТУ им. Г. И. Носова» был реализован **проект «Киберэкстремизму — нет!»**. *Целью проекта* являлась активизация профилактики киберэкстремизма в образовательных учреждениях посредством формирования активного неприятия экстремизма во всех его проявлениях учащимися школ и других учебных заведений Российской Федерации, помощь учащимся, учителям и родителям в ослаблении психологических предпосылок возникновения этих антисоциальных явлений.

*Основные задачи проекта:*

- Формирование у школьников, их родителей и учителей представлений:
  - о порочности экстремизма во всех его проявлениях как способа решения отдельных противоречий в сфере межнациональных и межконфессиональных отношений между людьми;
  - о несостоятельности терроризма как основного средства достижения целей политическими экстремистами.

*Таблица 5*

**Виды проектов по дисциплине «Информационная безопасность»**

| Вид проекта | Пример проекта |
|---|---|
| Практико-ориентированные или социально значимые проекты | Разработка учебного проекта по теме «Интернет: проблемы защиты интеллектуальной собственности» |
| | Разработка внеклассного мероприятия по теме «Вкусивши яд компьютерных игр...» |
| | Организационно-техническое обеспечение проведения олимпиады для школьников «Информационный щит» |
| | Разработка семинара для родителей по теме «Организация контентной фильтрации при работе в сети Интернет» |
| | Разработка учебного проекта по теме «Троянская война» («Как не получить троян от фишера со скидкой?» и др.) |
| Исследовательские проекты | Анализ состояния проблемы по обеспечению безопасности персональных данных в образовательном учреждении |
| | Исследование проблем формирования компьютерной этики и этикета, морально-этических норм поведения в виртуальной реальности |
| | Защита школьников от нежелательной информации в сети Интернет и др. |
| Управленческие проекты | Разработка проекта по обеспечению безопасности персональных данных в образовательном учреждении |
| | Управление рисками информационной безопасности образовательной инфраструктуры |
| | Разработка регламентов, правил информационной безопасности для пользователей информационно-образовательной среды |
| | Программа и политика информационной безопасности образовательного учреждения |
| Проекты по информационным системам | Проектирование и разработка электронного учебно-методического комплекса по модулю «Компьютерная этика и этикет» |
| | Разработка обучающе-контролирующей программы по теме «Родительский контроль в сети Интернет» |

- Содействие выработке у школьников, их родителей и учителей:
  - иммунитета к попыткам экстремистских кругов влиять на сознание граждан России;
  - психологической устойчивости перед проявлениями экстремизма и киберэкстремизма.
- Оказание влияния на предупреждение появления среди школьников, их родителей и учителей элементов экстремистских воззрений.

В ходе реализации проекта **разработано содержание специального модуля «Вопросы профилактики киберэкстремизма среди молодежи»**, позволяющего преподавателям вуза включить его в состав ряда читаемых дисциплин в бакалавриате. Включение данного модуля позволило ввести новые, остроактуальные темы в дисциплины «Информационная безопасность», «Информационная безопасность в системе открытого образования», «Информационная безопасность в образовании», «Информационные технологии в образовании», «Методика организации внеурочной деятельности по информатике и ИКТ», а также в систему послевузовского образования научно-педагогических кадров.

Особое внимание в ходе обучения нами было уделено **вовлечению студентов в научно-исследовательскую и проектную работу, связанную с вопросами обеспечения информационной безопасности в образовании**. Актуализирована тематика работы студентов, молодых ученых, преподавателей и аспирантов в соответствии с современным состоянием проблемы обеспечения информационной безопасности. Апробация результатов работы студентов осуществлялась посредством:

- выступления на конференциях различного уровня;
- проведения конкурса творческих работ;
- разработки проектов для школьников и студентов;
- организации круглых столов, диспутов и других мероприятий, посвященных изучаемой проблеме.

Студентами разработаны и реализованы во время прохождения педагогической практики учебные проекты по проблеме исследования для учащихся общеобразовательных школ.

В ходе реализации проекта организованы и проведены методические семинары для учителей общеобразовательных школ, педагогов системы дополнительного образования с целью включения в работу по профилактике вовлечения молодежи в киберэкстремистскую деятельность.

Материалы, полученные по результатам работы проектных групп, также используются в различных формах представления результатов:

- комплексные или индивидуальные курсовые/дипломные проекты;
- представление проектов на внешние конкурсы и гранты;
- студенческие научные работы, представляемые на конкурсы;
- публичная защита проектов в университете и/или в образовательном учреждении;
- подготовка публикаций по тематике проектов;
- выполнение курсовых и дипломных работ по сквозной тематике и др.

Как показал опыт применения активных методов обучения при формировании компетенций у будущих учителей в области обеспечения информационной безопасности, у студентов заметно повысилась мотивация, направленная на изучение и применение методов защиты информации; преподаватели отмечают положительное влияние методов на способности генерировать, структурировать и классифицировать идеи, собирать и анализировать информацию, предлагать альтернативные решения, эффективно взаимодействовать друг с другом, решать возникающие проблемы.

Предполагается дальнейшее широкое использование научного и методического результатов работы в образовательном процессе:

- обсуждение проблем формирования устойчивости личности к негативным формам воздействий в сети Интернет на занятиях с бакалаврами и магистрами, на методологических семинарах с аспирантами, молодыми преподавателями;
- модернизация и разработка новых учебных программ дисциплин высшего и послевузовского профессионального образования, курсов повышения научной и профессиональной квалификации с учетом научно-методических наработок исследования;
- введение новых тем по вопросам обеспечения информационной безопасности в образовательные программы в части регионального компонента и дисциплин по выбору для профильных специальностей и направлений высшего образования, системы послевузовского образования научно-педагогических кадров;
- актуализация тематики научно-исследовательской работы студентов, молодых ученых, преподавателей и аспирантов;
- использование материалов проекта при курсовом и дипломном проектировании и др.

Материалы работы предполагается использовать:

- при проведении НИР и НИРС со студентами, преподавателями вузов, при проведении конференций, круглых столов, заседаний научных школ и научных лабораторий;
- при написании учебников, учебных пособий для студентов, обучающихся по ИКТ-направлениям (педагогическое образование (профили «Информатика и экономика», «Начальное образование и информатика»), «Прикладная информатика», «Бизнес-информатика» и др.).

**Список использованных источников**

1. *Бьюзен Т., Бьюзен Б.* Супермышление: измените свою жизнь с помощью интеллект-карт. Минск: Попурри, 2014.

2. *Инашвили С. Я.* Применение кейс-метода при обучении будущих учителей информатики управлению рисками образовательных проектов с использованием веб-сервиса RiskGap // Эволюция, прогресс и модернизация: сборник научных трудов по материалам I Международной научно-практической конференции студентов, магистрантов и аспирантов. СПб.: НОО «Профессиональная наука», 2017.

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. Ч. 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. Ч. 3.

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

6. *Мусийчук М. В.* Философско-педагогический дискурс научно-популярной литературы о юморе // Мир науки. 2016. Т. 4. № 1.

7. *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.

8. *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.

9. *Недосекина А. Г., Чусавитина Г. Н.* Формирование эстетического идеала как средство профилактики киберэкстремизма // Фундаментальные исследования. 2014. № 12. Ч. 5.

10. *Овчинникова И. Г., Курзаева Л. В., Чусавитина Г. Н.* Профилактика киберэкстремизма в системе образования: базовые решения на основе компетентностного подхода // Фундаментальные исследования. 2013. № 10. Ч. 5.

11. *Чусавитин М. О., Чусавитина Г. Н.* Модель методики формирования у будущего учителя информатики компетенции в области обеспечения информационной безопасности // Новые информационные технологии в образовании: Материалы VII Международной научно-практической конференции. Екатеринбург: РГППУ, 2014.

12. *Чусавитина Г. Н.* Апробация организационно-педагогических условий повышения эффективности подготовки научно-педагогических кадров к обеспечению информационной безопасности в сфере электронного образования и науки // Новые информационные технологии в образовании: Материалы VI Международной научно-практической конференции. Екатеринбург: РГППУ, 2013.

13. *Чусавитина Г. Н., Давлеткиреева Л. З., Новикова Т. Б.* Анализ современного состояния исследований проблемы формирования у студентов университета устойчивости к технологиям негативного информационно-психологического воздействия в сети Интернет // Современные наукоемкие технологии. 2016. № 11-2.

14. *Чусавитина Г. Н., Зеркина Н. Н.* Профилактика киберэкстремизма в системе современной высшей школы как социальная проблема // Мир науки. Социология, филология, культурология. 2016. № 1.

15. *Чусавитина Г. Н., Курзаева Л. В., Давлеткиреева Л. З., Чусавитин М. О.* Подготовка будущих учителей к обеспечению информационной безопасности. Магнитогорск: МГТУ им. Г. И. Носова, 2017.

16. *Чусавитина Г. Н., Мусийчук М. В.* Педагогические аспекты проблемы противодействия угрозам в сети Интернет // Мир науки. 2017. Т. 5. № 6.

17. *Чусавитина Г. Н., Чернова Е. В., Макашова В. Н., Зеркина Н. Н., Кузнецова И. М.* Этические вопросы применения информационных технологий как компонента предметного содержания подготовки студентов университета // Фундаментальные исследования. 2015. № 10. Ч. 2.

18. *Чусавитина Г. Н., Чусавитин М. О.* Анализ проблемы готовности педагогических кадров к профилактике и противодействию идеологии киберэкстремизма среди молодежи // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи / под ред. Л. З. Давлеткиреевой, Г. Н. Чусавитиной, Е. В. Черновой. Магнитогорск: Магнитогорский государственный университет, 2013.

19. *Chernova E. V.* Teachers Training for Prevention of Pupils Deviant Behavior in ICT // Conference on Information Technologies in Science, Management, Social Sphere and Medicine (ITSMSSM-2016). Conference proceedings. Atlantis Press, 2016.

20. *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.

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

22. *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 (ITSMSSM-2016). Conference proceedings. Atlantis Press, 2016.

## Приложения

*Приложение А*

### Приемы использования ментальных карт

**Прием «Пустая карта».**

Обучающимся предлагается создать ментальную карту по определенной теме. В готовой ментальной карте находится только тема занятия (рис. А1).

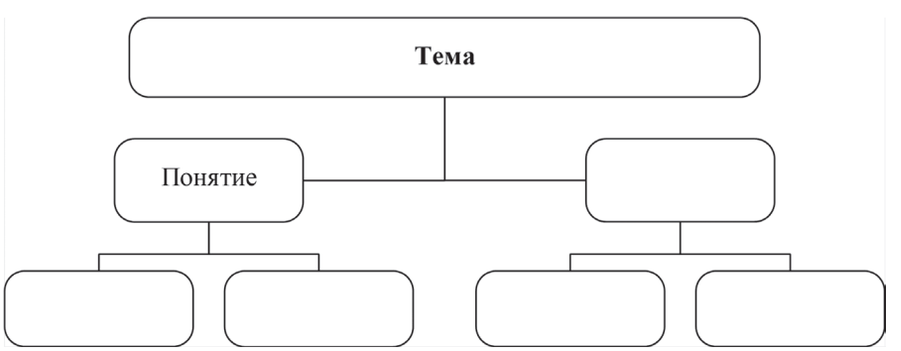


*Рис. А1. Прием «Пустая карта»*

**Прием «Ключевые понятия».**

На предложенной ментальной карте обучающиеся должны выделить основные понятия и установить взаимосвязи между понятиями (рис. А2).

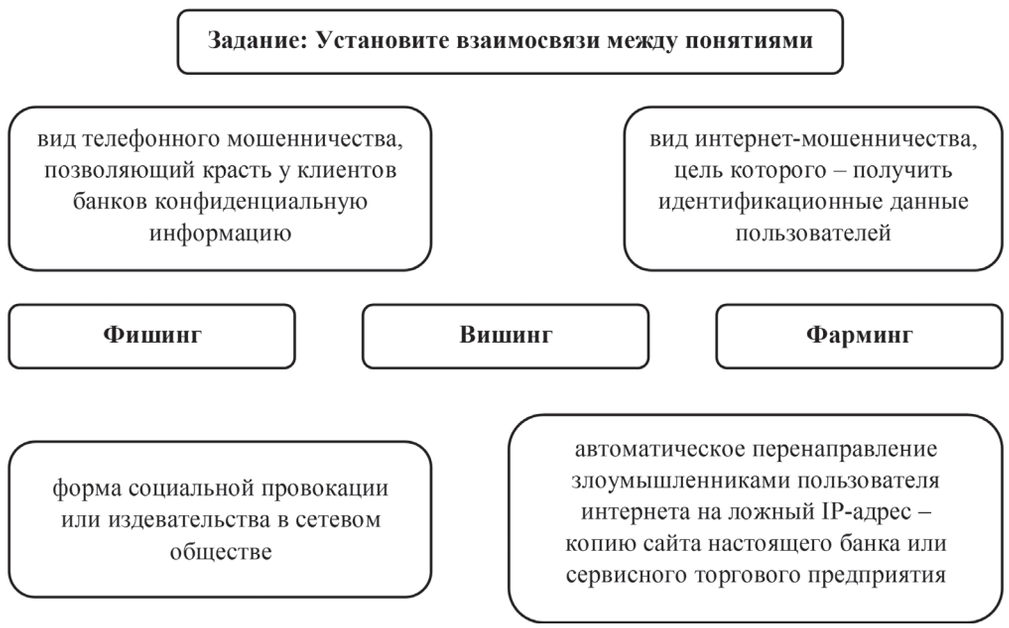


*Рис. А2. Прием «Ключевые понятия»*

**Прием «Заполнение».**

На составленной в сервисе ментальной карте студенты должны записать пропущенные ключевые термины (рис. А3).

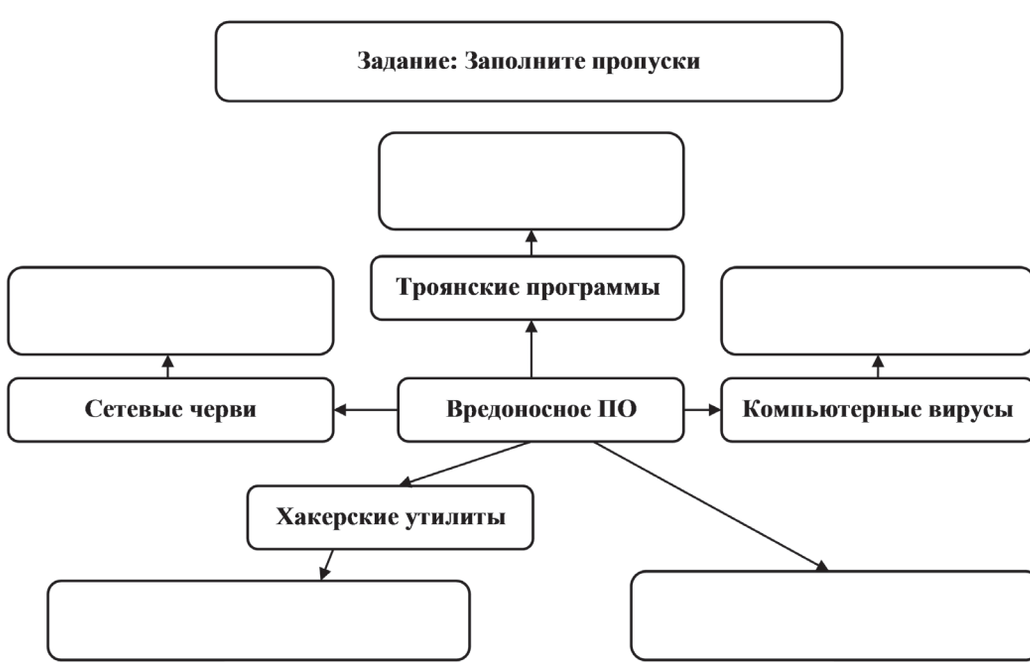


*Рис. А3. Прием «Заполнение»*

**Прием «Дополнение».**

Обучающиеся должны продолжить построение ментальной карты по одной или нескольким темам (рис. А4).


*Рис. А4. Прием «Дополнение»*

**Прием «Установи соответствие».**

Обучающимся предлагается установить соответствие терминов темы и их определений (рис. А5).


*Рис. А5. Прием «Установи соответствие»*

**Прием «Исправь ошибки».**

Обучающимся предлагается исправить ошибки в представленной ментальной карте (рис. А6).


*Рис. А6. Прием «Исправь ошибки»*

**Прием «Оживи карту».**

Обучающимся предлагается, используя как можно больше ассоциативных изображений, видеофрагментов, цветовых решений и пр., придать карте большую эмоциональную выразительность (рис. А7).

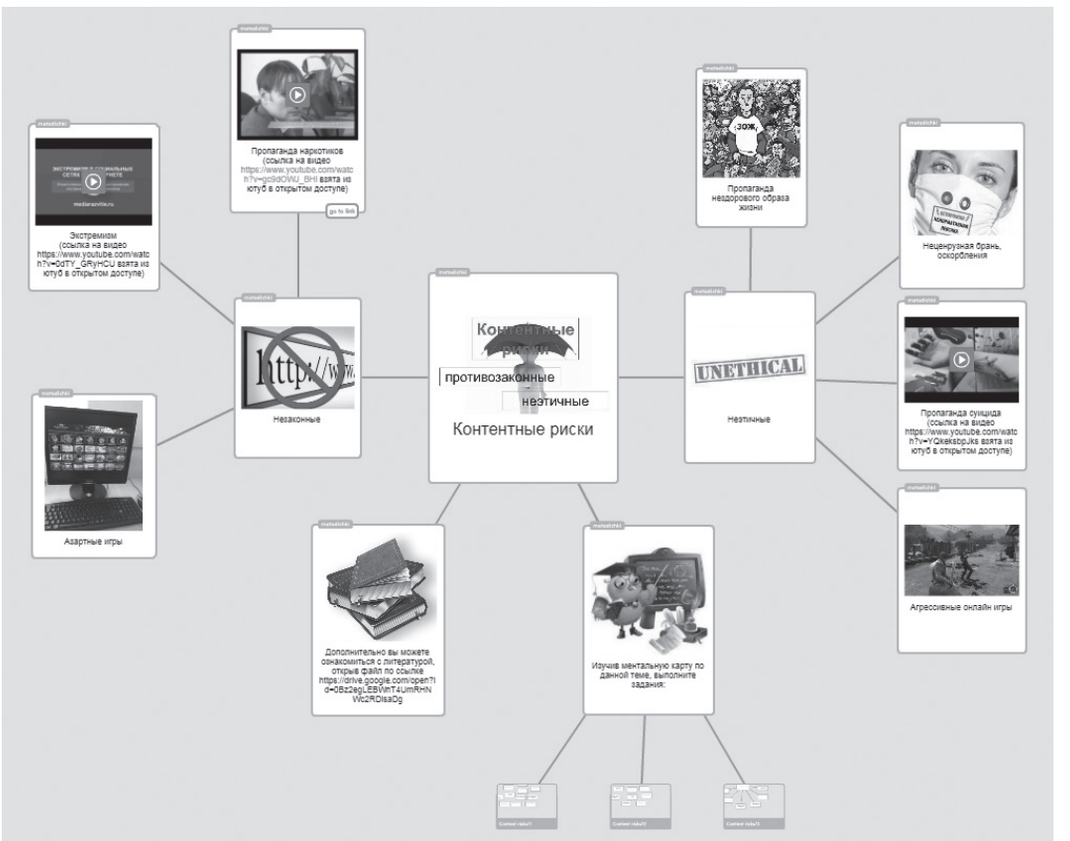


*Рис. А7. Прием «Оживи карту»*

**Прием «Что хотел сказать автор?»**

Обучающимся предлагается, используя предложенную ментальную карту, описать представленный на ней процесс, событие, идею или мысль автора.

ISSN 0234-0453 • ИНФОРМАТИКА И ОБРАЗОВАНИЕ • 2018 • № 1 (290)

**Анализ сервисов для создания ментальных карт**

| № п/п | Название сервиса | Необходимость регистрации на сайте | Приложение настольное/ облачное | Поддержка русского языка | Бесплатное создание ментальных карт | Наличие шаблонов | Бесплатное использование готовых шаблонов | Возможность загрузки изображений, видео | Возможность добавления гиперссылок на другие интернет-ресурсы | Совместное редактирование карты | Поддержка функции «чат» |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Coggle.it | + | Облачное | + | + | – | – | Только изображения | + | + | – |
| 2 | Cacoo | + | Облачное | + | В бесплатном режиме доступно 25 карт | + | + | + | + | + | + |
| 3 | MindMeister | + | Облачное | + | + | + | + | + | + | + | + |
| 4 | XMind | + | Настольное | + | + | – | – | + | + | + | – |
| 5 | MindManager | + | Настольное | + | 30 дней для бесплатного тестирования | – | – | + | + | + | + |
| 6 | Popplet | + | Облачное | + | + | + | + | + | + | + | – |
| 7 | FreeMind | + | Настольное | + | + | + | + | + | + | + | – |

**Примеры ментальных карт**

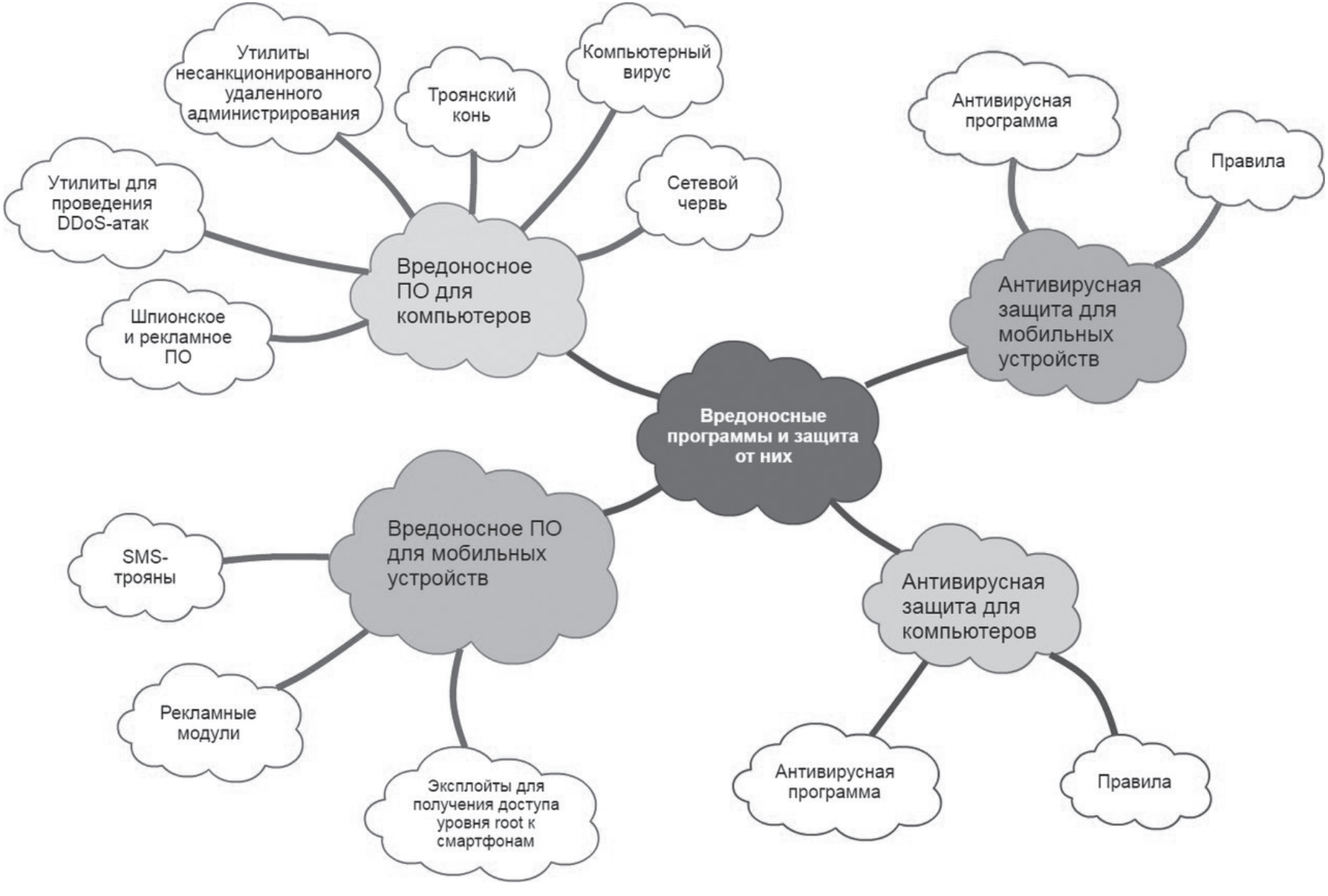


*Рис. В1. Ментальная карта «Виды вредоносных программ и методы защиты от них»*

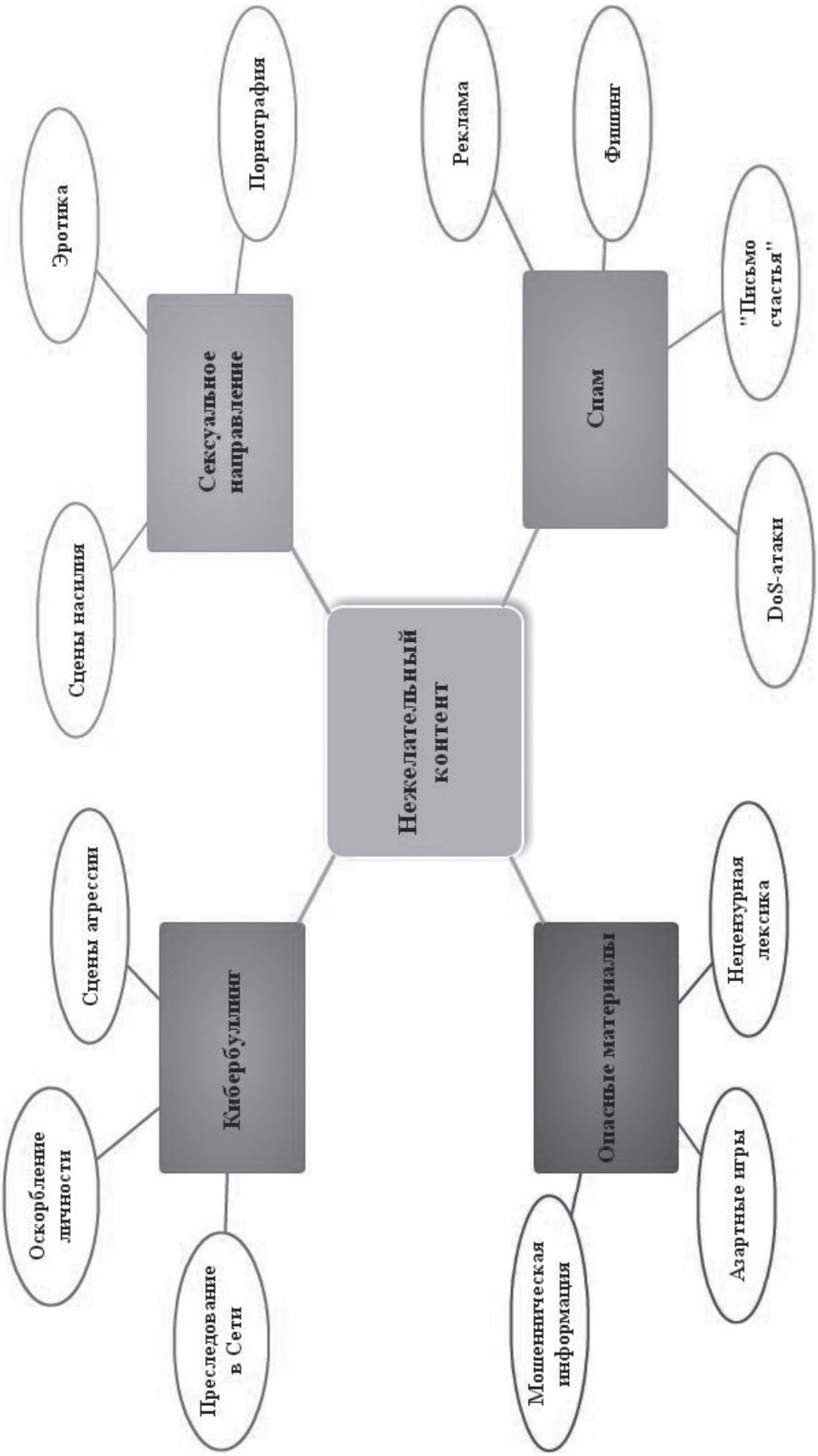


*Рис. В2. Ментальная карта «Виды нежелательного контента в интернете»*