

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное автономное образовательное учреждение
высшего образования «Национальный исследовательский
Нижегородский государственный университет им. Н.И. Лобачевского»

Р.В. Голубин
И.А. Исакова
А.П. Коротышев
П.П. Рыхтик

**КИБЕРБЕЗОПАСНОСТЬ ПОДРОСТКОВ В СЕТИ ИНТЕРНЕТ.
ПРОТИВОДЕЙСТВИЕ КИБЕРУГРОЗАМ**

Учебно-методическое пособие

Рекомендовано учебно-методической комиссией
факультета социальных наук
для студентов ННГУ, обучающихся по направлению
подготовки «Конфликтология»
(программа бакалавриата)

Нижегород
2022

УДК 364.1
ББК 60.5

**КИБЕРБЕЗОПАСНОСТЬ ПОДРОСТКОВ В СЕТИ ИНТЕРНЕТ.
ПРОТИВОДЕЙСТВИЕ КИБЕРУГРОЗАМ:** учебно-методическое пособие /
Р.В. Голубин, И.А. Исакова, А.П. Коротышев, Н.С. Косарева, П.П. Рыхтик. –
Нижний Новгород: Нижегородский госуниверситет, 2022. – 65 с.

Рецензент: заведующая кафедрой отраслевой и прикладной социологии
факультета социальных наук Нижегородского государственного университета
им. Н.И. Лобачевского, д.с.н., доцент И.Э. Петрова

Учебно-методическое пособие посвящено сетевым угроз безопасности
молодого поколения в пространстве, а также рассматривает возможности обу-
чения молодежи безопасному использованию виртуальной реальности и про-
тиводействия киберугрозам.

Учебно-методическое пособие содержит следующие разделы: цели
освоения дисциплины; структура и содержание; учебно-методическое обеспе-
чение занятий лекционного и семинарского типа; тексты лекций и планы тре-
нингов и деловых игр; рекомендации для организации самостоятельной ра-
боты обучающихся; списки основной и дополнительной литературы.

Пособие подготовлено в рамках проекта «Сетевая грамотность нижего-
родской молодежи: механизмы мониторинга и технологии развития» по реа-
лизации подпрограммы «Поддержка социально ориентированных некоммер-
ческих организаций в Нижегородской области» государственной программы
«Социальная поддержка граждан Нижегородской области», утвержденной по-
становлением Правительства Нижегородской области от 30 апреля 2014 г. №
298, при софинансировании Фонда президентских грантов.

Ответственный за выпуск:
председатель учебно-методической комиссии
факультета социальных наук ННГУ
к.б.н., доцент А.В. Орлов

УДК 364.1
ББК 60.5

© Нижегородский государственный
университет им. Н.И. Лобачевского, 2022

СОДЕРЖАНИЕ

Введение.....	4
1. Цель освоения курс	6
2. Структура и содержание курса	6
3. Учебно-методическое обеспечение занятий лекционного типа	7
4. Материалы для занятий лекционного типа	9
<i>Лекция 1 «Киберзависимость, вовлечение в сообщества»</i>	<i>9</i>
<i>Лекция 2 «Кибербуллинг и интернет-обусловленное поведение».....</i>	<i>19</i>
<i>Лекция 3 «Фишинг данных, навязывание товаров/услуг»</i>	<i>28</i>
<i>Лекция 4 «Поддельные товары, фейковые продажи, мошенничество в сети»</i>	<i>34</i>
5. Учебно-методическое обеспечение занятий семинарского типа.....	38
<i>Семинар 1 «Киберзависимость, вовлечение в сообщества»</i>	<i>38</i>
<i>Семинар 2 «Кибербуллинг и интернет-обусловленное поведение».....</i>	<i>41</i>
<i>Семинар 3 «Фишинг данных, навязывание товаров/услуг»</i>	<i>44</i>
<i>Семинар 4 «Поддельные товары, фейковые продажи, мошенничество в сети»</i>	<i>47</i>
6. Учебно-методическое обеспечение самостоятельной работы обучающихся	51
7. Фонды оценочных средств для аттестации по дисциплине	53
<i>Тест.....</i>	<i>53</i>
<i>Проект</i>	<i>55</i>
8. Учебно-методическое и информационное обеспечение курса	57
9. Материально-техническое обеспечение курса.....	61
Заключение	62
Приложение 1. Технологическая карта сетевых угроз.....	63

Введение

В XXI веке происходят существенные трансформации социальной реальности, обусловленные активным проникновением в общественные процессы новых информационных технологий. Формирование потребностей, интересов, взглядов, ценностей человека в целом обусловлено его деятельностью в информационной среде, и, в первую очередь, это касается молодого поколения как наиболее лояльного к различным новациям.

Цифровая грамотность является основой продуктивного безопасного использования цифровых технологий молодыми людьми. Отсутствие цифровой компетентности создает угрозу для физического и психологического здоровья, социального благополучия личности, ограничивает её в онлайн-коммуникации, в доступе к образовательному и развивающему контенту, подвергает опасностям кибермошенничества и кибертравли.

Курс «Кибербезопасность подростков в сети Интернет. Противодействие киберугрозам» обладает методическим и дидактическим потенциалом в сфере формирования навыков безопасного поведения в сети и противодействия киберугрозам.

В пособии освещаются четыре основные темы, посвященные различным киберугрозам: «Киберзависимость, вовлечение в сообщества», «Кибербуллинг и интернет-обусловленное поведение», «Фишинг данных, навязывание товаров/услуг», «Поддельные товары, фейковые продажи, мошенничество в сети».

Пособие состоит из нескольких разделов. Первый раздел посвящен учебно-методическому сопровождению занятий лекционного типа. Выбор материала раздела зависит от уровня информированности обучающихся о киберугрозах. Если уровень информированности – низкий, то обучающимся предлагаются тематические лекции. К каждой лекции, для повышения качества усвоения материала, разработаны специальные упражнения.

Если уровень информированности – высокий, то обучающимся достаточно краткой справки по теме, которая озвучивается в ходе тренинга. Материал для такого информационного сообщения также представлен в пособии.

Второй раздел посвящен учебно-методическому сопровождению занятий семинарского типа. По каждой из четырех тем пособия предлагается либо тренинг, либо деловая игра для выработки навыков оценки сетевых угроз и противодействия им.

Третий раздел посвящен организации самостоятельной работы и содержит задания для самостоятельной подготовки, позволяющие развить исследовательские умения и критическое мышление.

Четвертый раздел предлагает средства контроля полученных знаний и навыков. Для оценки знаниевой компоненты авторами разработан тест. Для оценки сформированности навыков – проектное задание. Реализация проектного метода позволяет не только обучить работать в команде, но и сформировать у обучающихся готовность нести личную ответственность за результаты своего труда.

В пособии представлены результаты авторских исследований. Ассоциация выпускников ННГУ, с помощью ученых факультета социальных наук, провела исследование уровня сетевой грамотности нижегородской молодежи. Его первый этап проходил осенью 2021 г. и включал опрос школьников и онлайн мониторинг в новых медиа. С 18 по 22 января 2022 г. состоялся опрос студентов университета, завершающий второй этап исследования. Всего было опрошено 90 молодых людей в возрасте от 13 до 21 года.

Данное пособие будет интересно для людей, работающих в области профилактики, педагогов, классных руководителей, школьных психологов, работников социальных и молодежных служб, а также для студентов профильных ВУЗов.

1. Цель освоения курс

Целью курса «Сетевые угрозы Рунета» является формирование у обучающихся целостного, системного представления о сетевых угрозах Интернет-пользователям, а также навыков их выявлять и эффективно им противостоять.

В рамках курса обучающиеся рассмотрят такие угрозы как киберзависимость, кибербуллинг, фишинг и кибермошенничество, узнают о различных методах выявления этих угроз, освоят навыки противостояния им и разработают собственные проекты по снижению влияния киберугроз на общественные отношения.

Дисциплина «Сетевые угрозы Рунета» является факультативом.

2. Структура и содержание курса

Общая трудоемкость курса составляет 1 зачетную единицу, 36 часов, из них 4 часа – занятия лекционного типа, 12 часов – занятия семинарского типа, 20 – самостоятельная работа.

Наименование и краткое содержание разделов и тем дисциплины	Всего часов	В том числе				Самостоятельная работа обучающегося, часы
		Контактная работа (работа во взаимодействии с преподавателем), часы, из них				
		Занятия лекционного типа	Занятия семинарского типа	Занятия лабораторного типа	Всего	
Киберзависимость, вовлечение в сообщества		1	2		3	4
Кибербуллинг и интернет-обусловленное поведение		1	2		3	4
Фишинг данных, навязывание товаров/услуг		1	2		3	4
Поддельные товары, фейковые продажи, мошенничество в сети		1	2		3	4
Презентация собственного проекта			4		4	4
ИТОГО		4	12		16	20

Занятия семинарского типа (практическая подготовка) предусматривают:

- анализ конкретной ситуации – кейса,
- участие в тренингах (выполнение упражнений),
- участие в деловых играх.

Текущий контроль успеваемости реализуется в рамках занятий семинарского типа.

Промежуточная аттестация проходит в традиционной форме – зачет.

3. Учебно-методическое обеспечение занятий лекционного типа

Процесс изучения дисциплины предусматривает ознакомление обучающихся с лекционными материалами. Основными темами курса являются «Киберзависимость, вовлечение в сообщества», «Кибербуллинг и интернет-обусловленное поведение», «Фишинг данных, навязывание товаров/услуг» и «Поддельные товары, фейковые продажи, мошенничество в сети».

В пособии предлагаются как аннотации лекций, так и полное содержание, выбор объема теоретического материала зависит от возможностей учебного процесса. При проведении отдельных тематических практических занятий можно ограничиться кратким теоретическим экскурсом с освещением ключевых вопросов, отраженных в аннотациях; при проведении полного цикла профилактических мероприятий необходимо воспользоваться текстом лекций.

Раздел подготовлен на основе авторской разработки «Технологическая карта сетевых угроз» – перечня сетевых угроз, классифицированных с точки зрения возможных последствий, степени опасности для молодежи Нижнего Новгорода.

Лекция 1 «Киберзависимость, вовлечение в сообщества»

Киберзависимость – это психосоциальная проблема, проявляющаяся в навязчивом желании использовать Интернет без контроля проведенного в нем времени, что приводит к разрыву или потере социальных связей с окружением и замене реальных отношений и интересов виртуальными.

Виды киберзависимости: Интернет-гемблинг, Интернет-гейминг, Интернет-хакерство, Интернет-шопоголизм, Интернет-серфинг, киберкоммуникативность.

Признаки киберзависимости: отказ от реального общения ради досуга в сети, раздражение в случае долгого отсутствия доступа к сети Интернет, конфликты по поводу использования компьютера и Интернета, пренебрежение правилами личной гигиены и распорядком питания, сна, потребность в бесцельном длительном потреблении информации в сети Интернет (некритичное длительное бесцельное чтение информации в Интернете).

Киберзависимость – это проблема, снижающая уровень коммуникативного, социального и эмоционального интеллекта подрастающего поколения.

Лекция 2 «Кибербуллинг и интернет-обусловленное поведение»

Интернет-обусловленное поведение – это совокупность действий и поступков, связанных с импульсами к действию, полученных индивидом в коммуникативном пространстве Интернета.

Интернет-обусловленное поведение характеризует изменения в психологических и поведенческих характеристиках молодых людей, использующих электронные средства коммуникации.

Кибербуллинг – это агрессивное преследование индивида с использованием цифровых технологий в течение продолжительного периода времени.

Кибермоббинг – это совокупность намеренных оскорблений, угроз, диффамации и публикаций с компрометирующими данными, осуществляемая с использованием цифровых технологий в течение продолжительного периода времени.

Кибербуллинг и кибермоббинг от традиционной травли отличает: анонимность преследователя; возможность постоянно преследовать жертву с разных аккаунтов; сокрытие жертвой фактов преследования от родителей и взрослых из-за страха ограничения доступа к Интернету; публичность травли, большое количество свидетелей; длительное сохранение в сети Интернет материалов травли; отсутствие действенных программ выявления случаев кибербуллинга; отсутствие программ наказания агрессоров.

Лекция 3 «Фишинг данных, навязывание товаров/услуг»

Фишинг – это вид интернет-мошенничества с целью получения логина и пароля для доступа к персональным данным, в том числе финансовым. В большинстве случаев фишинг представлен в виде массовых рассылок писем и уведомлений от известных брендов, почтовых систем, банков, социальных сетей. Мошенники размещают в письме логотип организации, сообщение и прямую ссылку на сайт, который не имеет внешних отличий от настоящего, на поддельном сайте требуется ввести конфиденциальные данные в соответствующие формы. Таким образом мошенники получают доступ к банковским счетам и учетным записям.

Виды фишинга: рассылка писем с вирусами, фарминг (секретное перенаправление пользователя на заражённый сайт без его ведома), смишинг (атаки с помощью смс), вишинг (атаки с помощью телефонных звонков) и др.

Фишинг-атака – это рассылка мошеннических сообщений с повышенной концентрацией и частотой на определенных площадках или каналах связи.

Способы противодействия фишинговым атакам: смена паролей, проверка источников информации, периодическая проверка аккаунтов, изучение информации о вредоносных программах.

Лекция 4 «Поддельные товары, фейковые продажи, мошенничество в сети»

Мошенничество – это хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием с использованием цифровых технологий.

Наиболее распространенными являются такие мошеннические практики, как фишинг (хищение личных данных), онлайн-продажи товаров и услуг, мошенничество в сфере интернет-банкинга.

Фишинг – это одна из наиболее распространенных форм мошенничества в Интернете, которая представляет собой способ хищения персональных данных при помощи фальсификации различных сайтов. Среди актуальных практик мошенничества в Интернете можно отметить букмекерские сайты и онлайн-казино, работающие по фишинговой схеме.

Интернет-попрошайничество также является известным видом мошенничества, которое выражается в просьбе пожертвовать некоторую денежную сумму. Алгоритм работы: это создать или «присвоить» аккаунт и просить деньги у пользователей. Такой вид мошенничества используется в социальных сетях, особенно популярны Facebook, Instagram, Telegram, Viber, WhatsApp, Вконтакте и Одноклассники.

Поддельные торговые сайты или интернет магазины – вид интернет-мошенничества, при котором, виновные создают клоны или зеркальные копии известных сайтов товаропроизводителей (используя логотип, шаблон дизайна веб-сайта и текст оригинального бренда и пр.), размещают объявления о продаже товаров. В дальнейшем, получив денежные средства, не выполняют своих обязательств по заключенному договору: не отправляют товар, либо отправляют товар гораздо худшего качества, чем было заявлено.

Брачные аферы – вид мошенничества, состоящий в том, что виновные, используя интернет-сайты знакомств, знакомятся после чего под различными предлогами (оплата стоимости проезда, оформление заграничного паспорта, визы и пр.), получают финансовую помощь от наивных потерпевших.

4. Материалы для занятий лекционного типа

Лекция 1 «Киберзависимость, вовлечение в сообщества»

Киберзависимость: определение, признаки и виды

Глобальная сеть Интернет как любой социальный феномен имеет как положительные стороны, так и отрицательные черты, одной из которых является возможность возникновения зависимости от неё.

Киберзависимость – это психосоциальная проблема, проявляющаяся в навязчивом желании использовать Интернет без контроля проведенного в нем времени, что приводит к разрыву или потере социальных связей с окружением и замене реальных отношений и интересов виртуальными.

Интересный факт:

Всемирная организация здравоохранения (ВОЗ) внесла зависимость от видеоигр в Международную классификацию болезней.

Термин «Интернет-зависимость» был впервые применен американским психиатром Иваном Голдбергом, он описал её как патологическое, непреодолимое влечение к использованию Интернета.¹

Одним из первых исследователей Интернет-зависимости можно назвать американского психотерапевта Кимберли Янг (Kimberley S. Young), она в 1994 г. разместила на одном из сайтов в сети Интернет тест для выявления Интернет-зависимых лиц. Интернет-зависимость она описывает, как навязчивое желание выйти в Интернет, находясь «offline» и неспособность выйти из Интернета, будучи «online». К. Янг описывает Интернет-зависимость, как с точки зрения ее психологических аспектов, так и социальных отношения с родителями, друзьями, врачами, коллегами по работе и учебе.

Киберзависимость – это психосоциальная проблема, которая приводит к разрыву или потере социальных связей с ближайшим окружением и замене реальных отношений и интересов виртуальными, в связи с этим у человека изменяется сознание, поведение и способ решения социальных проблем.

Интересный факт:

В январе 2022 г. в России насчитывалось 129,8 млн. интернет-пользователей. Среднестатистический житель России проводит в Интернете 7 часов 50 минут в сутки и практически половина (47%) этого времени – в мобильном устройстве.

Интересный факт:

По данным исследования Superjob, проведенного в 220 российских городах в 2021 г.:

- 42% россиян считают, что у них есть интернет-зависимость: 11% – однозначно уверены, что находятся в состоянии интернет-зависимости, 31% – скорее уверены;
- женщины чаще мужчин признавались, что испытывают зависимость от интернета: 43% женщин и 40% мужчин.

Чрезмерное увлечение гаджетами, Интернетом и социальными сетями может приводить к серьезным нарушениям здоровья. Первое возможное последствие – появление проблем со зрением. Второе последствие – поражение нервных стволов руки, связанные с перенапряжением мышц, который ведет к синдрому запястного канала. Третье последствие также является от длительного сидения за компьютером – остеохондроз и сколиоз. Четвертое последствие – облучение от компьютера, приводящее к нервным перегрузкам, головным болям и расстройствам сна. Чрезмерное увлечение виртуальным миром может приводить к нарушениям в эмоционально-психологической сфере: уныние, апатия и депрессия могут возникать из-за несоответствия «идеального», «иллюзорного», виртуального мира с действительностью, понижается творческая активность.

¹ Агеева, Н.А. Особенности Интернет-зависимых личностей / Н.А. Агеева // Вестник Российского университета дружбы народов. – 2007. – №1. – С. 73-74.

Ключевыми признаками киберзависимости являются²:

- потеря контроля над временем, проводимом в сети;
- навязчивое желание проверить свои профили (электронная почта, аккаунт в социальной сети) в Интернете;
- сужение зоны интересов – потеря интереса к другим видам досуга;
- агрессия при попытке прекратить Интернет-сеанс или ограничить доступ к сети Интернет, конфликты с окружающими по поводу времяпрепровождения в глобальной сети;
- предпочтение виртуальной реальности действительной – отстранение от окружения, потеря контактов с людьми в «оффлайне»;
- бесцельное потребление информации – блуждание по веб-сайтам без конкретной цели;
- отказ от реального общения ради досуга в сети;
- покупка новых устройств и программного обеспечения, покупка различных премиум аккаунтов в Интернете и др.

Стоит отметить, что современный Интернет является динамично развивающейся средой. Коммуникационные возможности постоянно расширяются, порождая, помимо полезных возможностей, новые разновидности киберзависимости.

Кибергеймомания – это зависимость от онлайн-игр, являющаяся самой опасной формой зависимости от Интернета. Это связано с тем, что человек, вживаясь в роль персонажа игры, может полностью отключиться от реального мира, для него может присутствовать только мир, созданный компьютером. Это может привести к дезориентации в реальном пространстве, когда индивид путается в том, что реально, а что нет. Геймомания характеризуется полным отсутствием ответственности и в мнимой возможности исправить любую ошибку.

Интересный факт:

По данным авторского исследования:

- ❖ 75% подростков отмечают, что они не ощущают потребности в увеличении времени, проводимого в сети;
- ❖ 89% замечают за собой, что проводят намного больше времени в Интернете, чем предполагали.
- ❖ 40,4% опрошиваемых иногда ощущает раздражительность и беспокойство при отсутствии возможности использовать социальные сети;
- ❖ 10% опрошенных часто ощущают раздражительность и беспокойство при отсутствии возможности использовать социальные сети;
- ❖ 20% подростков не имеют других хобби, кроме онлайн-игр;
- ❖ 13,2% – используют Интернет как постоянный метод решения личных проблем;
- ❖ 54,3% – игнорирует домашние обязанности ради того, чтобы дольше побыть в Интернете;
- ❖ 17% подростков не знают лично своих виртуальных друзей;
- ❖ у 83% подростков круг онлайн-знакомств пересекается с их реальной жизнью.

² Гайнцев Е.Г. Анализ Интернет-зависимости и механизм её формирования / Е.Г. Гайнцев// Российский электронный научный журнал. – 2014. – №5. – С. 58-59.

Одной из разновидностей кибергейминга является кибергемблинг – это патологическая склонность к азартным играм в сети Интернет, заключается в частых повторных эпизодах участия в азартных играх, которые ведут к снижению социальных, профессиональных, материальных и семейных ценностей. Вовлеченность в таких занятиях гораздо выше, чем в онлайн-играх, потому что здесь есть возможность быстро выиграть денежные призы. Популярность кибергемблинга объясняется легкой доступностью к ресурсам казино, скрытность, иллюзия «легкого заработка», высокая разрекламированность.

Киберкоммуникативность – это зависимость, связанная с общением в социальных сетях. Главным побочным эффектом является перенос реального живого общения в виртуальную среду Интернета. Притягательность социальных сетей заключается в возможности создавать и редактировать свой образ и идентичность согласно собственным желаниям, одновременно общаться с большим количеством людей, получать практически мгновенную реакцию на свои посты и сообщения. Возможность сохранять свою анонимность и дистанцированность от собеседника в сети позволяет смелее, чем в реальной жизни, выражать не только положительные, но и отрицательные эмоции.³

Интернет-серфинг – это зависимость от поиска информации в сети, которая заключается в бесконтрольном просмотре как можно большего количества веб-страниц за минимально короткое время. Люди тратят много времени на поиск, сбор и структурирование информации из Интернета, однако из-за больших объемов сведения практически не усваиваются (запоминаются только отдельные факты), нарушаются когнитивные схемы в мозге. И вместо развития, происходит торможение умственной деятельности.

Интернет-шопоголизм – это компульсивное влечение к покупкам в сети Интернет. Отличие обычного шопинга от компульсивного в том, что потребитель покупает целенаправленно, то, в чем есть потребность, четко осознавая стоимость товара и размер своего дохода, а шопоголик руководствуется желанием купить даже то, что ему не нужно, важен сам процесс покупки, при котором цена и сумма потраченных средств не учитываются.

Популярность кибершопинга объясняется особенностями сети Интернет: покупки можно совершать в любое время (круглосуточно), скрытно (без посещения магазина); выбор товаров не ограничен (доступны магазины всего мира); деньги списываются из онлайн-кошелька (т.е. нет визуализации при расходовании денег, не видно «пустеющий кошелек»); возможен выход за рамки личных границ (можно без стеснения купить любой товар). Таким образом, кибершопоголизм – это хроническое навязчивое стремлением делать ненужные покупки в Интернет-магазинах в неконтролируемых количествах. Шопоголизму более подвержен женский пол, однако и мужчины рискуют «заразиться кибершопоголизмом», утратив рациональное мышление при очередной трате денежных средств.

³ Богданова О.А. Интернет-зависимость у детей и подростков / О.А. Богданова // Вестник МГПУ. – 2014. – №1(27). – С. 55.

Итак, киберзависимость, как и любая другая, начинает проявляться не сразу. Постепенное вовлечение в сеть Интернет сопровождается определенными признаками и симптомами, которые можно отследить. Значимым является то, что молодые люди не осознают, что так сильно вовлечены в виртуальную реальность, заменяющую живое общение и жизненный опыт по преодолению трудностей.

Технологии вовлечения в сообщества

Развертывание в социальных сетях массовых маркетинговых или информационно-пропагандистских кампаний также требует специфических технологий:

1. «Тренд». Информационная шумиха, внезапная популярность, возникающая вокруг события или некой тематики. Обычный цикл популярности новости в интернете занимает 3 дня: в течение первого она приобретает высокую популярность, затем в течение двух следующих, постепенно исчезает из информационной повестки. Но новость, попавшая (или усиленно продвигаемая) в тренд остается в центре общественного внимания гораздо дольше, иногда до нескольких лет.

В основе тренда, как интернет-технологии, лежит достаточно давно использовавшийся в СМИ метод «перепечатки» (или, в современной интернет-терминологии, «расширивания»)⁴. Он предусматривает наращивание информации путем простого ее воспроизводства с минимальными изменениями исходного контента (не более 20% от исходного содержания). Это служит также и способом поддержки популярности контента при недостатке новых информационных поводов. Широкому применению данного метода дополнительно способствует тот факт, что подобные действия в РФ не классифицируются, как нарушение авторского права⁵.

Интересный факт:

По данным авторского исследования:

- внимательно следят за развитием социально-политических событий – 36,6% опрошенных;
- читают об этом, только если случайно натыкаются на информацию – 51,5%;
- однако о событии, которое все обсуждают, 90% опрошенных ищут информацию целенаправленно. Это и есть эффект тренда.

Интересный факт:

По данным авторского исследования:

- 22,2% молодых людей склонны доверять сообщениям блогеров и видеоблогеров;
- 28,1% – не склонны им доверять;
- 49,7% – не определились с ответом.

⁴ Тимофеев А.А. Цитирование новостей в печатных СМИ и интернет-изданиях: правовые аспекты // Медиа-скоп. – 2012. – №1. – С. 17.

⁵ Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 N 14-ФЗ (ред. от 29.07.2018) (с изм.

Однако тренд, как более совершенная технология, обладает также и свойством «самоподдержания». Чем более популярным становится тренд, тем большее число субъектов интернет-коммуникации (блогеров, постеров, интернет-СМИ и др.) присоединяется к его раскрутке. На определенном этапе тематику тренда просто невозможно игнорировать – субъектам приходится реагировать на популярную повестку, а их читатели и подписчики напрямую требуют реакции на тренд.

При этом, участие в обсуждении и продвижении тренда вовсе не означает искренней поддержки его идей. Многие делают это только потому, что популярная тема придаст и популярности и им. Через несколько недель раскрутки тренда уже невозможно понять, где его реальные сторонники, а кто просто накручивает себе просмотры.

Наконец, отметим, что тренды зачастую возникают вокруг деструктивных общественных явлений, поскольку эмоционально-окрашенные негативные события привлекают людей больше, нежели позитивные.

Интересный факт:

Внимание молодежи к информационным сообщениям достаточно ограничено по времени:

- 20,8% опрошенных забывают новость, как только прочитают;
- 26,4% отслеживают материал «2-3 дня, пока новость в топе»;
- и только 29,2% – следят за информацией до логического финала.

Интересный факт:

По данным авторского исследования:

- 20,9% опрошенных всегда прислушиваются к мнению блогеров при выборе товара;
- 44,4% делают это время от времени;
- 34,6% полагаются на свое мнение.

Тренд неизменно привлекает к себе общественное внимание и служит важным информационным ориентиром для современной молодежи. Ее внимание привлекают самые обсуждаемые события, молодые люди готовы совершать дополнительные действия (искать информацию, мониторить социальные сети) ради того, чтобы быть «в курсе». Однако интерес к отдельным информационным поводам удерживается довольно короткое время, что показывает несколько «поверх-

ностное» отношение к получаемой информации, и является проявлением «клипового» типа мышления. Эти социально-психологические особенности молодежи делают ее уязвимой для технологий продвижения тренда, применяемых как в коммерческих целях, так и для политической пропаганды.

2. «Хайп» – действия отдельных субъектов коммуникации по привлечению к себе повышенного внимания с целью повышения своего медийного капитала (т.е., проще говоря, своей узнаваемости). В социальных сетях и видеохостингах он выражается в виде, например, числа подписчиков, просмотров и лайков. Чем больше подписчиков, просмотров и лайков набирает аккаунт,

тем легче и выгоднее ему размещать рекламу, привлекать донаты, продвигаться в топ.

В отличие от тренда, который существует «объективно» и поддерживается многочисленными субъектами, хайп всегда строго привязан к своему автору. Собственно, цель хайпа и состоит в повышении личной узнаваемости. Поскольку речь для авторов хайпа идет о том, чтобы выделиться из общества, они, в большинстве случаев, идут по пути нарушения общественных норм.

Технология хайпа эксплуатирует особую функцию СМИ, которую П. Лазерсфельд обозначил как «присвоение статуса»⁶. Выступая источником хайпа, его субъекты становятся лидерами мнений, к чьим посланиям и точкам зрения аудитория как минимум прислушивается, а порой и некритически принимает на веру.

Влияние точки зрения блогеров на молодежь столь значительно, что они могут формировать устойчивый интерес к какой-либо теме: после просмотра роликов/ленты блогеров, 81% опрошенных продолжает дополнительно искать информацию по той же проблеме. То есть, можно констатировать высокую лояльность молодежи к авторитетам в Сети и, соответственно, высокую эффективность технологии хайпа.

3. «Воронка». В коммерческом интернет-продвижении воронка служит в качестве инструмента отбора целевой аудитории. В этом качестве она и нередко заимствуется и теми группами, что преследуют в интернете политические цели.

К примеру, она с успехом применялась радикальными исламскими течениями для вербовки сторонников. Механизм отбора следующий: из крупной группы, выражающей широкий круг интересов (к примеру, группы об исламской культуре) ссылки ведут в более мелкую группу с конкретизированным содержанием (к примеру, группу, оказывающую помощь пострадавшим в конфликтах мусульманам), а из нее – в небольшую группу, содержащую уже откровенно противоправный контент (к примеру, вербовку наемников-ислаμισлов). С теми, кто прошел отсев до конечной группы работают уже в офлайн режиме.

Таким образом, достигаются две цели. С одной стороны, происходит постоянный отбор пользователей по заданному алгоритму. С другой, конечную группу легко скрыть и не жалко потерять. Модераторы социальных сетей регулярно удаляют конечные группы за противоправный контент, но основная воронка продолжает действовать, поскольку в ней нет ничего незаконного. На создание же новой конечной группы, вместе со ссылками у опытного пользователя уходит около трех минут.

⁶ Personal Influence: The Part Played by People in the Flow of Mass Communications / By Elihu Katz and Paul F. Lazarsfeld. With a Foreword by Elmo Roper. A Report of the Bureau of Applied Social Research, Columbia University. – Glencoe, Ill: The Free Press, 1955. – P. 34-45.

Общая схема работы воронки контента



Воронка может служить действенным механизмом мобилизации общества. Для любой социальной инициативы требуется активное меньшинство – ядро, вокруг которого будут объединяться сторонники тех или иных идей. Их отбор и первоначальная координация – достаточно сложная задача, которую и помогает успешно решать «воронка».

В заключение раздела заметим, что социальные сети представляют собой сложную, динамично меняющуюся систему. Их коммуникационные возможности постоянно расширяются, порождая, помимо полезных возможностей, новые формы киберугроз. Однако их основной функцией остается манипулирование мнением, как отдельных пользователей, так и больших социальных групп, с целью извлечения прибылей.

*Интерактивное задание к лекции «Киберзависимость,
вовлечение в сообщества»*

Упражнение 1: задача обучающихся проработать предлагаемые им тексты статей.

Работа будет вестись в соответствии с технологией развития критического мышления, методом ИНСЕРТ (I.N.S.E.R.T. – «Interactive Notation System for Enhanced Reading and Thinking»)⁷.

ИНСЕРТ – это метод чтения текста, которое сопровождается маркировкой информации с использованием значков:

V – это я знал;

+ – новая информация;

– – противоречит моим представлениям;

? – информация непонятна или недостаточна.

По мере чтения значки ставятся на полях справа. На чтение текста отводится 15 минут.

Ход упражнения:

1) Обучающиеся делятся на группы по 4 человека. Каждая группа получает по статье (для удобства чтения, каждой группе обучающихся, выдается по две одинаковые статьи).

Список статей для чтения обучающихся:

1. Сорокина К.О. Современное состояние проблемы индивидуально-психологических особенностей личности подросткового возраста с киберзависимостью / К.О. Сорокина // E-Scio. – 2020. – № 5(44). – С. 727-732. [Электронный ресурс] – URL: <https://www.elibrary.ru/item.asp?id=42988994>

2. Васильева Ю.Е. К вопросу о проблеме интернет-зависимости в современном обществе / Ю.Е. Васильева, И.А. Ивашина, П.П. Попов, И.Г. Рыжов // Прикладные информационные аспекты медицины. – 2014. – Т. 17. – № 1. – С. 48-51. [Электронный ресурс] – URL: <https://www.elibrary.ru/item.asp?id=21357604>

3. Мамедов А.К. Подросток в системе «Человек-Машина»: интернет-аддикция и девиантные формы поведения / А.К. Мамедов // Миссия конфессий. – 2021. – Т. 10. – № 7(56). – С. 727-741. [Электронный ресурс] – URL: <https://www.elibrary.ru/item.asp?id=47631562>

4. Левин Л.М. Психофизиологические и психиатрические аспекты интернет-зависимости / Л.М. Левин // Научное мнение. – 2020. – № 5. – С. 68-78. [Электронный ресурс] – URL: <https://www.elibrary.ru/item.asp?id=43100895>

5. Шайкина Е.А. Технологии профилактики компьютерной зависимости личности / Е.А. Шайкина // Педагогика и психология: теория и практика. – 2015. – № 2(2). – С. 30-38. [Электронный ресурс] – URL: <https://www.elibrary.ru/item.asp?id=32476078>

⁷ Грудзинская Е.Ю., Марико В.В. Активные методы обучения в высшей школе. Учебно-методические материалы по программе повышения квалификации «Современные педагогические и информационные технологии». – Нижний Новгород, ННГУ, 2007. – 182 с. – С. 20.

6. Максименко С.Д. Проблема виртуальной зависимости у подростков / С.Д. Максименко, А.С. Лысенко // Психиатрия, психотерапия и клиническая психология. – 2020. – Т. 11. – № 2. – С. 265-278. – DOI 10.34883/PI.2020.11.2.004. [Электронный ресурс] – URL: <https://www.elibrary.ru/item.asp?id=44101232>

2) Обучающиеся читают тексты с помощью метода ИНСЕРТ.

3) Закончив читать, участники должны нарисовать и заполнить «Маркировочную таблицу», в каждую колонку которой следует внести не менее 3-4 пунктов.

V	+	-	?

Закончив заполнять таблицу, участники должны поделиться в группе своими впечатлениями, особенно следует обсудить, то что помечено «-» и «?». На это отводится 7-8 минут.

Далее происходит совместное обсуждение, в ходе которого преподаватель поясняет все вопросы, на которые обучающиеся не могут ответить сами. Обсуждение продолжается до тех пор, пока все сложные моменты не прояснятся.

Упражнение 2. Круглый стол «Киберзависимость – миф или болезнь?»

В основе этого метода лежит принцип коллективного обсуждения проблем, изучаемых в системе образования. Обучающиеся должны научиться выступать в роли докладчиков и оппонентов, владеть умениями и навыками постановки и решения интеллектуальных проблем и задач, доказательства и опровержения, отстаивать свою точку зрения, продемонстрировать достигнутый уровень теоретической подготовки.

Главная цель занятия состоит в том, чтобы обеспечить обучающимся возможность практического использования теоретических знаний о киберзависимости и возможностях ее профилактики.

Эффективность семинара во многом зависит от качества выполнения обучающимися Упражнения 1.

Ход упражнения:

1) Обучающиеся располагаются за круглым столом.

Преподаватель также должен находиться в кругу с обучающимися.

2) Краткое вводное слово преподавателя, включающую формулировку темы и цели круглого стола.

3) Далее перед участниками ставится вопрос – киберзависимость – это болезнь или нет?

- 4) Развертывание дискуссии.
- 5) Выработка согласованных позиций по предмету обсуждения.

В заключении подводятся итоги работы «круглого стола», высказываются пожелания его участникам и присутствующим.

Лекция 2 «Кибербуллинг и интернет-обусловленное поведение»

Кибербуллинг: понятие, признаки, виды

Современный Интернет представляет собой огромный информационный банк, основы использования которого разнообразны: пользователь может создавать и распространять любой контент, как позитивный, так и нейтральный, и даже негативный. Кибербуллинг – это совершенно новая форма хулиганства, ставшая возможной благодаря увлеченности и опыту молодежной культуры компьютерными технологиями.

Травля или буллинг (англ. bullying) – это агрессивное преследование члена коллектива со стороны другого человека либо группы лиц.

Травля – это вид психологического насилия, эмоционального давления, преследования, возможно даже с элементами физического насилия и унижения.

Кибербуллинг – это намеренный и неоднократный вред, причиненный посредством использования компьютеров, мобильных телефонов и других электронных устройств⁸.

Кибербуллинг – это агрессивное преследование индивида с использованием цифровых технологий в течение продолжительного периода времени.

В социологической литературе любая травля рассматривается как социальное взаимодействие с целью запугивания; физический или психологический террор, направленный на то, чтобы вызвать у другого страх и тем самым подчинить его себе.

По мнению социолога Е.Н. Ожиевой, травля – это умышленное, длительное, повторяющееся физическое или психологическое насилие со стороны индивида или группы, которые имеют определенные цели (физические, психологические, административные и т.д.) относительно жизни другого человека, и которое происходит преимущественно в коллективах.⁹

С развитием информационных и коммуникационных технологий Интернет стал новой площадкой для травли. Первое определение «кибербуллингу»

Интересный факт:

По данным аналитического центра компании Microsoft в 2016 г. 65% взрослых и подростков заявили, что они становились объектами травли.

⁸ Hinduja, S., & Patchin, J. W. / Bullying beyond the schoolyard: Preventing and responding to cyberbullying. – 2009. – Thousand Oaks, CA: Corwin Press.

⁹ Ожиева Е. Н. Буллинг как разновидность насилия. Школьный буллинг. [Электронный ресурс] / Е.Н. Ожиева. – URL: http://www.rusnauka.com/33_NIEK_2008/Psihologia/37294.doc.htm (дата обращения 20.02.2022)

дал канадский педагог Билл Белсеем. Он считает, что кибербуллинг – это использование информационных и коммуникационных технологий, например, электронной почты, мобильного телефона, личных интернет-сайтов, для намеренного, неоднократного и враждебного поведения лица или группы, направленного на оскорбление других людей.¹⁰

Кибербуллинг может включать такие действия:

- создание угроз,
- посылка провокационных, расовых или этнических оскорблений,
- попытка заразить компьютер жертвы вирусом,
- заполнение почтового ящика сообщениями (спам),
- публикация заведомо ложных сведений о жертве,
- разглашение личных данных.

Ведущие исследователи кибербуллинга в России – Г.У. Солдатова и А.Н. Ярмина – так описывают ролевую структуру кибербуллинга – это социальное взаимодействие агрессора, жертвы, помощников агрессора и помощников жертвы, а также пассивных наблюдателей.¹¹

Киберагрессоров закономерно отличает высокий уровень интернет-активности и использования мессенджеров для обмена сообщениями, проблемное поведение в офлайне (целенаправленная порча имущества, контакты с полицией, физическое нападение на членов семьи, кражи, употребление сигарет или алкоголя). Киберагрессоры имеют заниженную самооценку, низкий уровень эмпатии, самоконтроля, высокий уровень импульсивности, агрессивное чувство юмора.

У кибержертв часто выявляется проблема с самооценкой, чувство одиночества и отсутствия социальной поддержки, более высокий уровень выраженности депрессивных симптомов, переживания гнева и печали, психосоциальные проблемы, проблемы в отношениях в семье, отчужденность, внешняя враждебность. Помимо этого, для кибержертв характерны более высокий уровень тревоги и стресса.

Интересный факт:

По данным авторского исследования:

- 47% сталкивались с негативными комментариями в Интернете;
- 27% сталкивался с неуважением границ личной жизни: кто-то распространял тайны или личную информацию в сети Интернет;
- 11% приходилось писать негативные комментарии по поводу чего-то или замечания кому-то в Интернете;
- 28% убеждены, что в Интернете они могут писать и говорить все, что хотят;
- 25% школьников сталкивались с проблемой кибербуллинга.

¹⁰ Belsey B. Cyberbullying: An Emerging Threat to the «Always On» Generation [Электронный ресурс] – URL: <https://billbelsey.com/?cat=13> (дата обращения: 10.02.2022).

¹¹ Солдатова Г.У., Ярмина А.Н. Кибербуллинг: особенности, ролевая структура, детско-родительские отношения и стратегии совладания // Национальный психологический журнал. 2019. №3 (35) [Электронный ресурс] – URL: <https://cyberleninka.ru/article/n/kiberbulling-osobennosti-rolevaya-struktura-detsko-roditelskie-otnosheniya-i-strategii-sovladaniya> (дата обращения: 26.02.2022).

Нередко те, кто травят других онлайн, сами становятся жертвами травли или – наоборот.

Поведение наблюдателей в ситуациях кибербуллинга иногда можно описать эффектом свидетеля или, как его еще называют, – синдромом Дженовезе – это психологический эффект, проявляющийся в том, что люди, ставшие свидетелями какого-либо негативного происшествия, не пытаются помочь пострадавшему. Причем, чем больше наблюдателей становятся невольными свидетелями такой ситуации, тем меньше шансов, что кто-то из них вмешается и попытается помочь. Анонимность в Интернете может позволяет наблюдателям игнорировать собственную совесть.

Таким образом, данные эмпирических исследований показывают, что традиционная ролевая структура буллинга претерпевает значительные изменения в связи с опосредствованием травли информационно-коммуникационными технологиями.¹²

Кибербуллинг и традиционная травля также отличаются тем, что:

➤ кибербуллинг не связан с физическим насилием, давление происходит только психологическое, эмоциональное.

➤ кибербуллинг связан с кажущейся анонимностью агрессора. При обычной травле жертва видит агрессора, а социальные сети позволяют сохранять условную анонимность. Под «условной анонимностью» понимается сложность выявления отправителя послания, однако развивающиеся программные средства при должном количестве усилий позволяют вычислить агрессора. Этот процесс сложнее, чем в реальной среде, однако возможный.

➤ кибербуллинг – явление круглосуточное, так как может происходить в любое время дня и ночи;

➤ агрессор и жертва могут не находиться рядом территориально. Возможности сети Интернет позволяют травить жертву независимо от места жительства, т.е. переезд в данном случае не решит проблему насилия;

➤ кибербуллинг происходит при большом количестве свидетелей за счет неограниченного круга наблюдателей – множества пользователей сети Интернет;

➤ агрессор не осознает тяжесть вреда, который наносит жертве, поскольку буллинг опосредован техническими средствами, и он не видит, как плохо жертве от неприятных комментариев.

Рассмотри самые распространенные формы травли в интернете:

Киберфлейминг – это обмен эмоциональными сообщениями в социальных сетях, между двумя и более людьми, содержащими оскорбления.

Троллинг – форма социальной провокации или издевательства в сетевом общении по средством публикации информации, которая вызывает у жертвы чувство тревоги, сильную эмоциональную реакцию. Агрессор ощущает чувство могущества над эмоциональным состоянием жертвы.

¹² Солдатова Г.У., Ярмина А.Н. Кибербуллинг: особенности, ролевая структура, детско-родительские отношения и стратегии совладания // Национальный психологический журнал. 2019. №3 (35) [Электронный ресурс] – URL: <https://cyberleninka.ru/article/n/kiberbulling-osobennosti-rolevaya-struktura-detsko-roditelskie-otnosheniya-i-strategii-sovladaniya> (дата обращения: 26.02.2022).

Хейтинг – это публикация необоснованная критика в адрес другого человека.

Секстинг – это публикация и распространение фото и видео с обнаженными и полуобнаженными людьми.

Киберсталинг – это преследование или домогательство с помощью Интернета.

Фрэпинг – это форма социальной провокации, когда человек создает «фейковую» страницу или аккаунт и выдает себя за другого человека, используя его фотографии, личную информацию для размещения нежелательного контента.

Грифёрство или грифинг – это нанесение морального и материального ущерба людям в компьютерных играх.

Диссинг – это публикация и рассылка унижительной информации, с целью порчи репутации или нанесения вреда взаимоотношениям с близкими людьми. Это могут быть искаженные фотографии, часто имеющие сексуальный характер, портящие репутацию человека.

Для предотвращения и профилактики попадания в ситуацию буллинга необходимо проведение просветительских мероприятий, направленных на распространение и разъяснение учащимся, родителям сведений о кибербуллинге, правилах поведения в интернет-пространстве. Родители часто объясняют детям, как общаться с незнакомыми людьми на улице, но редко – как это делать в Интернете. Родители должны способствовать установлению с детьми отношений эмоционального принятия, доверия, поддержки и т.д.

Интересный факт:

По данным авторского исследования:
➤ 52,6% – не сталкивались с неприятными сообщениями или комментариями в сети, 25,2% – иногда, 22,1% – часто;
➤ 71% школьников сообщили бы о фактах издевательств наиболее близким людям.

В случае обнаружения первых признаков онлайн-травли нужно немедленно обратиться к администратору сообщества или веб-сайта с просьбой удалить нежелательный контент; не отвечать на подозрительные сообщения, повысить сложность паролей своего профиля, не передавать/не публиковать личные данные, заблокировать агрессора.

Интернет-обусловленное поведение

В жизни современного человека социальные сети играют важную, а порой и основополагающую роль. Их успех и широкое распространение объясняется тем, что они отвечают глубинным социально-психологическим мотивам человека, таким как:

- Потребность в коммуникации. Пользователи устанавливают контакты, обмениваются информацией, общаются. При этом негативную информацию и неприятных собеседников можно легко «отсечь» одним кликом.

- Потребность в социализации. Пользователи объединяются в сообщества по интересам, получают одобрение единомышленников, чувствуют свою принадлежность к группе. На пространстве социальных сетей легко почувствовать собственную важность и симпатию других.

- Потребность в самопрезентации. Интерфейс социальных сетей позволяет легко создавать у других иллюзию собственной успешности, показывать свою жизнь такой, какой хочет ее видеть пользователь.

- Потребность в самоидентификации. Человек склонен сравнивать себя с другими людьми, в особенности с теми, кто имеет с ним много общих черт. На основе этого формируется его самооценка.

- Потребность в развлечении. Социальные сети предоставляют широкий круг виртуальных развлечений, которые, в отличие от радостей реальной жизни, не требуют физических усилий или финансовых затрат.

В то же время, общение в социальных сетях лишено социальных рисков: с виртуальными собеседниками можно не церемониться, и за критику оппонента он автора к ответу не призывает. Если же оппонент наскучил, или начал брать верх в споре, его можно заблокировать и забыть навсегда. Поэтому на пространстве социальных сетей люди зачастую ведут себя так, как никогда не рискнули бы вести себя в реальной жизни. На этом, главным образом, и строится представление о социальных сетях как о пространстве свободного общения.

Социальные сети выполняют также и ряд важных общественных функций. Они служат для общественной коммуникации, поддержания культурных связей, распространения новых идей, играют роль дискуссионной площадки, несут развлекательную функцию.

Однако следует помнить, что *основная задача социальных сетей, для выполнения которой они и создавались, это коммерческие продажи.*

В основу здесь положен достаточно простой принцип. Любой бизнес-проект для успешного старта продаж требует, в первую очередь, определения целевой аудитории. Прежде чем что-то продавать, необходимо выяснить: кто этим интересуется, что ему нравится, где и когда он готов это купить. Затем, для массовых продаж, нужно завладеть вниманием этих людей, выделить их из общей массы, привлечь в свои магазины.

До появления социальных сетей этим целям служили обширные маркетинговые исследования. Они требовали огромных финансовых затрат, обширного штата экспертов и многочисленных сотрудников, опрашивавших людей на местах. Такое могли позволить себе лишь крупные корпорации и торговые

Интересный факт:

По данным авторского исследования:
Среди молодых нижегородцев:

- 24,8% проводят в социальных сетях более 6 часов;

- 19,8% – 5-6 часов;

- 22,8% – 3-4 часа в день.

- 63,4% опрошенные не могут представить свою жизнь без Интернета.

- 45,5% отметили, что у них есть проблемы, которые легче обсудить онлайн, чем при живом общении.

сети. Множество бизнес-стартапов разорялось из-за того, что их авторы не могли верно оценить свою нишу рынка и подстроить под нее логистику и продажи.

Социальные сети представляют, в этом отношении, уникальный инструмент. Огромные массы потребителей сами вносят себя в общую базу данных, сами предоставляют информацию о себе, сами разбиваются на целевые группы по интересам, сами предоставляют свои контакты для рекламы и продаж. Администрация социальных сетей собирает эти сведения, сводит в пакеты данных и продает коммерческим структурам. На их основе строятся стратегии продаж, рекламные кампании, планы продвижения новых брендов и т.д.

Отсюда следует, что *в социальных сетях не существует некоммерческого контента.*

Даже если вы выкладываете в сеть фото любимого котика, это означает, что вы подняли кому-то продажи или хотя бы просмотры, выступили объектом маркетингового исследования, помогли разработать рекламную стратегию и пр.

Главная задача социальных сетей: организация таргетированных (т.е. нацеленных на конкретные ниши рынка и группы покупателей) продаж. Однако их возможности могут использоваться для распространения любой информации, как конструктивного, так и деструктивного свойства. На пространстве социальных сетей можно встретить:

1. Продажи самых разнообразных, в т.ч. поддельных товаров.
2. Субкультурные сообщества самой различной направленности.
3. Антигосударственную и политическую пропаганду.
4. Коммерческие психокульты, эксплуатирующие идеи личностного роста, позитивного мышления, саморазвития и пр.
5. Деструктивные религиозные сообщества.
6. Группы, пропагандирующие опасный досуг, деструктивное и асоциальное поведение, суицид и т.п.

Некоторые из этих угроз описаны в настоящем пособии. Однако этот контент очень разнообразен, круг создаваемых им угроз безопасности постоянно меняется. На место хорошо изученных и описанных угроз постоянно приходят новые.

Поэтому, в рамках развития сетевой грамотности, имеет смысл изучать не конкретные угрозы, а методы и технологии их продвижения.

Интересный факт:

Некоторые ученые утверждают, что секрет популярности котиков в интернете – нереализованный материнский инстинкт пользователей. По общему строению морда кота напоминает лицо новорожденного: большие глаза, покатый лоб, вздернутый нос. Такие пропорции подсознательно вызывают у человека симпатию.

Так это или нет, но каждое видео с котами в среднем набирает на YouTube 12 000 просмотров – больше, чем любой другой контент.

Естественно, это массово используется для рекламы и продвижения.

Пolemические приемы «интернет-троллей»

Операторы мультиакков, как и опытные «интернет-тролли», владеют обширным арсеналом полемических приемов. Используемые в интернет-дискуссии, они способны сбить неподготовленного человека с толку, заставить изменить свое мнение. Рассмотрим наиболее распространенные из них:

1. Инверсия, или внушение по принципу инверсии. В комментариях или постах формулируется тезис, противоположный тому, который оператор имеет целью доказать или внушить.

К примеру, если операторы продвигают какие-то формы социальной активности (флеш-моб, опасный досуг, психокульт и т.п.), они часто пользуются формулой «Только в интернете и можете писать, а вот я уже...» (зарабатываю Х рублей в мес., успешно совмещаю работу и досуг, достиг позитивного мышления и пр.).

Это – всегда провоцирующее утверждение. Оно призвано распалить внутреннюю гордость пользователя, заставить его написать ответ, обличающий неправоту отправителя, вступить с ним в полемику. Если пользователь зайдет достаточно далеко по пути отрицания позиции оператора, он может действительно принять участие в том, что тот рекламирует.

2. Псевдозапрет. Несколько иные формулировки характерны для технологии запрета. Она используется для провокации пользователя на определенное действие через высказывание прямого запрета на него. Например, «Вам ни в коем случае нельзя принимать участие в выборах».

Столкнувшись с любыми типами запретов, пользователь нередко демонстрирует склонность их нарушать. Особенно, когда сам запрет фактически воспринимается им как необоснованный или несостоятельный. К тому же, среди пользователей социальных сетей обычно распространены идеи о свободах и, в особенности, свободах виртуального пространства, где следует избегать появления формальных или неформальных запретов. Все это стимулирует в пользователях желание нарушать любых виды запретов на словах, а у некоторой части – и на деле.

Технологии инверсии и запрета очень примитивны. Подобные типы провокации очень часто встречаются в общении детей младшего школьного возраста (например, по принципу «взятия на слабо»). Впоследствии, в ходе взросления и расширения опыта межличностного общения, такие типы внушения обычно становятся бесполезны. Однако, масса пользователей сети воспринимает поступающую информацию не с рациональных позиций. Они продолжают ориентироваться на чувства и эмоции, а потому такой тип манипуляции все еще способен оказать достаточный эффект.

3. Риторический вопрос. Третьей манипулятивной технологией выступают тексты, представляющие собой вопрос, ответ на который, казалось бы, очевиден и общеизвестен. Для такого утверждения выбирается позиция, разделяемая большинством пользователей социальной сети или конкретного онлайн сообщества.

«Вы же хотите победить свои страхи? Тогда нужно...», «Вы же хотите, чтоб ваши дети были здоровы? Тогда обязательно...», «Хочешь поднять бабла? Давай...» и пр.

Цель подобных сообщений заключается в привязке целевого тезиса к позиции большинства. С ним не будут спорить, в силу нежелания опровергнуть устоявшееся мнение. А если и будут, всегда можно отвечать: «Да Вы просто в плену своих страхов», «Вы просто не думаете о детях», «Да ты просто неудачник» и т.д.

4. Импликация. Это – полемический прием, когда о желаемой позиции или мнении говорится вскользь, как о свершившемся факте, и сразу добавляется информация, отклоняющая дискуссию в стороннюю сферу.

Например, «Большинство из здесь присутствующих хотят купить новый смартфон, но как выбрать из всего многообразия?». С первой частью сообщения (о том, что новый телефон вообще нужен) спорить будут единицы.

Велика вероятность, что дискуссия пойдет по пути, предложенном во второй части сообщения, особенно если эмоционально он выглядит «ярче» или содержит провокационную точку зрения. Разгорятся споры, обсуждение моделей, и у пользователя действительно может появиться желание сменить телефон, которого изначально и не было.

5. Псевдотрюизм. С нежеланием противоречить условному большинству связана и схема манипуляции с использованием псевдотрюизма. «Трюизм» – использование в общении очевидных банальностей или общепринятых истин. Псевдотрюизм подразумевает использование придуманных истин или ссылку на сфабрикованное мнение популярного авторитета.

Такие сообщения могут звучать как: «Чем лучше человек понимает себя, тем больше он зарабатывает» или «Еще Аристотель говорил о необходимости развивать свое Я». В крайнем случае, можно просто выдавать свою позицию за банальность: «Известно, что ...».

6. Конфликтующая информация. Данный тип манипуляции, хотя формально и прост, требует многоплановой работы по распространению сообщений в определенный момент времени. Результатом работы становится появление в социальной сети большого массива утверждений, прямо противоречащих друг другу: например, по линии «надо идти на выборы» - «на выборы ходить нельзя»

Впрочем, эффект конфликтующей информации может возникать и естественным образом, когда интернет-аудитория разделена на несколько групп с принципиально разными взглядами, транслируемыми посредством постинга. В 2021-2022 гг. наиболее впечатляющим примером такого рода было интернет-противостояние прививочников и антипрививочников.

Основной смысл технологии в том, чтобы сломать сложившееся у членов определенного виртуального сообщества мнение по какому-либо вопросу. Целью здесь является запутать пользователя, потребляющего, но не успевающего анализировать большие объемы противоречивой информации. Это ведет к появлению у пользователя сомнений в истинности ранее усвоенного мнения.

Интерактивное задание к лекции «Кибербуллинг и интернет-обусловленное поведение»

Упражнение 1: сбор ассоциаций о кибербуллинге.

Упражнение проводится в форме «мозгового штурма».

Метод «мозговой штурм» (мозговой штурм, мозговая атака, [англ. brainstorming](#)) – это способ решения проблемы на основе стимулирования творческой активности, при котором участникам обсуждения предлагают высказывать как можно большее количество идей, в том числе самых фантастических. Затем из общего числа высказанных идей отбирают наиболее удачные.¹³

«Мозговой штурм» («мозговая атака») – это групповая дискуссия, которая характеризуется отсутствием критики поисковых усилий, сбором всех вариантов решений, гипотез и предложений, рожденных в процессе осмысления какой-либо проблемы, их последующим анализом с точки зрения перспективы дальнейшего использования или реализации на практике.¹⁴

Этапы проведения «мозгового штурма»:

1. Постановка и осмысление проблемы.

Преподаватель задает тему – «Ваши ассоциации со словом «кибербуллинг»» и предлагает высказать все ассоциации, которые вызывает слово «кибербуллинг».

2. Собственно, «мозговой штурм», генерирование идей.

Генерирование идей начинается с подачи преподавателем сигнала о начале работы. Студенты формулируют любые пришедшие им в голову идеи, стараясь избавиться от их критической оценки. Для этого преподаватель поощряет интеллектуальную активность участников, запрещает любые комментарии в адрес высказанных идей, блокирует невербальные эмоциональные реакции членов группы на услышанное, работа ведется в максимально быстром темпе. Каждому студенту слово предоставляется на несколько секунд, по очереди. Обучающиеся называют слова, преподаватель фиксирует их на доске и контролирует ситуацию, чтобы каждый студент назвал хоть одно слово.

3. Анализ полученных идей.

Этот этап носит характер групповой дискуссии, из которой исключены моменты персонализации выдвинутых предложений. Обсуждаются записанные на доске слова, полученные идеи сортируются на различные группы, предлагаемые как преподавателями, так и студентами, например, положительные черты или отрицательные и т.п. Следует отметить, что студенты должны работать даже с теми вариантами, которые им не нравятся, важно рассортировать всё. Оценка может носить не только качественный, но и количественный характер.

¹³ [Стариков П.А.](#) Пиковые переживания и технологии творчества: учебное пособие. – Красноярск: филиал НОУ ВПО «[Санкт-Петербургский институт внешнеэкономических связей, экономики и права](#)» в г. Красноярске, 2011. – 92 с. – С. 74-75.

¹⁴ Реутова Е.А. Применение активных и интерактивных методов обучения в образовательном процессе вуза (методические рекомендации для преподавателей Новосибирского ГАУ). – Новосибирск: Изд-во, НГАУ, 2012. – 58 с. – С. 11.

4. Обобщение результатов «мозгового штурма».
Преподаватель резюмирует сказанное.

Упражнение 2: составить текст, посвященный тому, чтобы убедить человека перестать травить другого, используя стратегию РАФТ.¹⁵

«РАФТ» – это вид творческой письменной работы, предполагающей проведение учащихся через процедуру «Роль – Аудитория – Форма – Тема» (РАФТ).

Шаги стратегии РАФТ:

1. Выбор темы. В данном занятии она задана – «Остановить киберагрессора».
2. Выбор роли. Роль (жертва, полиция, учитель, родитель и т.п.) (кто?) – От чьего имени вы будете писать письмо?
3. Выбор аудитории. Аудитория (кому?) – Кому Вы будете рассказывать? К кому обращена Ваша речь? Кто адресат? Агрессор, семья агрессора, класс, родительское собрание и т.п.
4. Выбор формы. Форма (как? в какой форме?) – Как Вы будете говорить? Какие подберете слова и выражения? Каким будет тон рассказа? Каков жанр истории?
5. Тема (о чем?) – О чем письмо? Каково его содержание?
Напишите письмо.
Объем итогового текста – не менее двух страниц.

Лекция 3 «Фишинг данных, навязывание товаров/услуг»

Интересный факт:

Персональные данные – это любая информация, прямо или косвенно относящаяся к физическому лицу, и позволяющая его определить.

Интернет, представляя одномоментно и пространство коммуникации, и площадку для потребления разнопланового контента, становится, в том числе, зоной утечки персональных данных. В современных реалиях на пользователей сети постоянно накладываются ограничения по взаимодействию между собой или по доступу к определенным источникам сетевой информации, в случаях, если они не прошли так называемые процедуры «регистрации» или «аутентификации». В конечном итоге это привело к нормализации в пользовательском сознании ситуации, когда на любом сайте, от официального правительственного портала, до небольшого *лэндинга*¹⁶ магазина по продаже, например, воздушных шаров,

¹⁵ Груздинская Е.Ю., Марико В.В. Активные методы обучения в высшей школе. Учебно-методические материалы по программе повышения квалификации «Современные педагогические и информационные технологии». – Нижний Новгород, ННГУ, 2007. – 182 с. – С. 40.

¹⁶ Маленький, одностраничный сайт, посвященный одной узкой теме и основной задачей которого, в большинстве случаев, является сбор контактных данных пользователя.

от них запрашивают какую-либо персональную информацию. Этой особенностью Интернета пользуются различного рода мошенники, стремящиеся заполучить персональные данные пользователей.

Фишинг данных – это особый тип методик по добыче персональных данных пользователей Интернета, основанных не на технических уязвимостях электронных устройств, а на особых приемах коммуникации «охотника за данными» и его «жертвы». Эти методики обычно имеют целью убедить жертву добровольно передать стороннему пользователю свои персональные данные, в связи с чем базируются на различного типа социально-психологических особенностях пользователей.

Интересный факт:

Лица, охотящиеся за пользовательскими данными по методикам фишинга, очень тщательно подходят к своей «работе», а простые пользователи сети очень редко бывают готовы к встрече с ними. По оценкам аналитиков уже в начале XXI века 70% фишинговых атак в различных социальных сетях были успешны для злоумышленников.

На данный момент с точки зрения законодательства РФ под «персональными данными» понимается буквально любое сочетание ФИО и какой-нибудь другой информации о человеке. Тем не менее, в большинстве случаев термин «фишинг» употребляется для обозначения ситуаций, когда злоумышленники стремятся овладеть персональными данными в корыстных целях. *Например, когда стремятся выяснить все данные банковской карты пользователя, с целью последующего снятия с карты всех доступных денежных средств.*

Юридической проблемой, связанной с подобными действиями злоумышленников, является тот факт, что такие действия формально не являются незаконными, а само понятие «фишинга» (или аналогичное ему) не закреплено в законодательных актах¹⁷. Это приводит к тому, что задачи сопротивления методикам фишинга лежат на плечи самих пользователей. Но успешное распознавание мошеннической схемы или хотя бы зарождение подозрения в использовании таковой требует или изначально специфического склада характера пользователя, или наличия у него осведомленности о конкретных приемах фишинга. Для успешного и комплексного противодействия подобного рода мошенникам необходимо проводить специальные просветительские мероприятия, а также регулярно распространять среди пользователей сети информацию о различных актуальных схемах фишинга.

Наконец, от всех пользователей требуется выработка персональной привычки подвергать сомнению любую информацию в сети и особенно в ситуациях, когда от них требуют озвучить, ввести или сфотографировать свои персональные данные. Ведь успешное противодействие охотнику за данными возможно только если пользователь распознал или заподозрил фишинг до момента передачи своих данных.

¹⁷ Батюшкин М.В. «Фишинг» – компьютерное мошенничество? // Символ науки. – 2021. – №1. – С. 90-93.

Распространенные методики фишинга данных и возможные средства противодействия им:

Методики	Противодействие
<p align="center"><i>Использование копий официальных сайтов</i></p> <p>Мошенниками используются сайты, крайне похожие на официальные сайты известных организаций, но служащие только для целей сбора персональной информации пользователей. Подобные сайты обычно называют «фишинговыми».</p> <p><i>Создать поддельный сайт (например, скопировав его код через команду в браузере «Ctrl» + «U») в современном мире становится все проще. Хотя сайты многих крупных компаний и содержат в своем коде элементы, противодействующие этому.</i></p> <p><i>Просто изобразить правдоподобный на вид сайт тоже редко требует большого труда.</i></p>	<p>Если пользователь собирается ввести на сайте любую информацию о себе, необходимо всегда уделить время для проверки данных сайта. Наиболее частым признаком фишингового сайта являются опечатки в домене (изменение букв или добавление к ним лишних символов) или просто странно сформулированный домен.</p> <p>Следующим признаком может быть странно составленная контактная информация, например, обилие одинаковых цифр в номере телефона или ОГРН. Если же просто вбить в поисковик «Яндекс» представленный на сайте телефон, ИНН или ОГРН, можно убедиться, как в подлинности самого номера, так и в его принадлежности конкретной организации. Сайты, не содержащие никаких контактных данных организации, рекомендуется игнорировать.</p>
<p align="center"><i>Ссылка на «авторитет»</i></p> <p>В начале общения мошенник ссылается на свою принадлежность к известному пользователю или универсальному социальному «авторитету» или институту. Например, представляется сотрудником государственной структуры (Пенсионный фонд, МВД и т.п.) или коммерческой организации (банк), к которой неким образом относится пользователь. Этот прием создает у пользователя иллюзию безопасности, что приводит к некритическому восприятию просьбы о предоставлении своих данных.</p>	<p>В ситуациях, когда запрос данных от «авторитетной» для пользователя структуры происходит, когда коммуникацию с ним в сети начал представитель структуры, но не пользователь данные предоставлять <i>не рекомендуется никогда</i>. Мошенник может быть очень убедителен и даже бывает способен предоставить правдоподобные доказательства своей принадлежности к «авторитету». Требуется прервать общение и связаться с представителем «авторитета» по официальным контактам, представленным на его официальном сайте.</p>

<p><i>Даже банальное подтверждение своей личности на запрос может обернуться проблемой, особенно если банк пользователя использует биометрические (голосовые) данные для аутентификации.</i></p>	
<p style="text-align: center;"><i>Тревожность</i></p> <p>Если на просторах сети пользователь столкнулся с информацией, вызывающей у него психологический дискомфорт или тревожность, скорее всего он становится жертвой социально-психологической манипуляции. Следующий в след за данной информацией запрос персональных данных имеет высокие шансы оказаться успешным.</p> <p><i>Люди склонны остро реагировать на информацию, намекающую на скорую или свершившуюся потерю денежных средств. Например, внезапно возникшая на экране фраза «Ваша карта заблокирована» способна встревожить подавляющее большинство пользователей.</i></p>	<p>Следует критически отнестись к любой информации в сети, если она вызывает у пользователя тревожность. Данная рекомендация очевидна и формально проста, но на практике требует от пользователя серьезных волевых усилий. Желательно тренировать сопротивление тревожности при помощи психологических тренингов, а также вести в своих заметках список тем, провоцирующих у пользователя беспокойство и помнить о необходимости критического анализа при столкновении с этими темами.</p> <p>Принимать решение о предоставлении в сети кому-либо или в какой-либо форме своих персональных данных на фоне психологического беспокойства нельзя.</p>
<p style="text-align: center;"><i>Сжатие сроков</i></p> <p>В охоте за данными злоумышленник стремится создать у пользователя ощущение, что на принятие решения у него очень мало времени.</p> <p><i>Сокращение сроков для проявления реакции на проблему/вызов – стандартный признак кризисной ситуации. Сталкиваясь с ограничениями по времени, люди склонны воспринимать ситуацию «кризисной», что психологически провоцирует некритическое восприятие информации.</i></p>	<p>Если в ходе коммуникации в сети у пользователя создается впечатление, что время на принятие какого-либо решения у него крайне ограничено, следует немедленно остановить коммуникацию и проанализировать ситуацию. Если процесс сопровождается требованиями предоставить персональную информацию о себе, высока вероятность того, что пользователь столкнулся с мошеннической схемой.</p>

<p style="text-align: center;">Соккрытие текста</p> <p>Многие автоматизированные системы противодействия фишинговым методикам (например, антивирусы или алгоритмы поисковых систем) подразумевают анализ текстов. Для обмана таких систем мошенники часто размещают текст запроса на персональные данные в виде картинки или высылая ссылку на сторонний от защищенного сайта/соц.сети ресурс, где уже содержится запрос на данные.</p>	<p>Следует всегда пробовать выделять текст любого запроса на персональные данные. Если текст невозможно выделить при помощи курсора или он расположен не на основном сайте/в социальной сети, а на «побочном» ресурсе, высока вероятность того, что пользователь столкнулся с попыткой фишинга его данных.</p>
--	--

Все методики чаще всего применяются в совокупности, использование только одной методики в ходе фишинга скорее исключение.

Проблема навязывания товаров или услуг пользователям сети

В сети пользователи часто приобретают различные товары, заказывают услуги или оформляют подписки на онлайн-сервисы. Иногда в этом процессе продавцы могут прямо или косвенно принуждать пользователя к приобретению дополнительного товара или услуги. Особенно просто со стороны продавца становится осуществлять подобное навязывание, поскольку в сети пользователь имеет дело или с еще не наблюдаемым непосредственно товаром или с буквально виртуальным-нематериальным продуктом (например, платный доступ к сайту). В этой ситуации «эфемерность» покупки заставляет пользователя некритично подходить к процессу торговли в Интернете. Тем более это усугубляется при все большем распространении практики онлайн-платежей, психологически нивелирующей и материальность денег в глазах пользователя.

Практики, принуждающие к покупке чего-либо, особенно в дополнение к необходимому пользователю товару, называются «навязыванием товаров или услуг» и прямо запрещены законодательством Российской Федерации¹⁸.

Противодействие таким практикам подразумевает соблюдение ряда рекомендаций:

- обращать внимание на присутствие в выставляемом сайтом счете, чеке или ином платежном документе сторонних (побочных) товаров или услуг и до момента оплаты четко обдумывать для себя их необходимость;

- не совершать в Интернете покупки на крупные суммы в тот же момент, когда произошло первое получение информации о данном товаре или услуге. Желательно брать паузу на обдумывание покупки, в идеале до нескольких дней. Особенно, если речь идет не о товарах или услугах первой необходимости.

¹⁸ Закон РФ от 07.02.1992 N 2300-1 (ред. от 11.06.2021) "О защите прав потребителей".

*Интерактивное задание к лекции «Фишинг данных,
навязывание товаров/услуг»*

Упражнение 1. «Фишинг данных – это»

Индивидуальная и коллективная работа с несколькими определениями рекламы.

Студенты читают различные определения фишинга:

– Фишинг – это вид интернет-мошенничества, используемого чтобы получить идентификационные данные пользователей.

– Фишинг – это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.

– Фишинг – это массовые рассылки писем и уведомлений от имени известных брендов, банков, платежных систем, почтовых сервисов, социальных сетей, в которых содержится форма для ввода личных данных через которую мошенники получают доступ к аккаунтам и банковским счетам пользователей.

– Фишинг – это получение путем обмана или методами социальной инженерии (хакерства с использованием человеческого фактора) персональных данных для использования в корыстных, преступных целях.

Обучающиеся знакомятся с этими определениями, выделяют слова, которые кажутся им ключевыми для определения фишинга. Затем начинается коллективная работа – на флипчарте в столбик записываются выделенные обучающимися ключевые слова.

Если это слово уже было названо, то рядом с термином ставится черточка. Таким образом, оценка может носить не только качественный, но и количественный характер.

Когда все студенты в группе высказались, все слова записаны, преподаватель вместе со студентами формулирует новое определение фишинга, употребляя все слова из списка.

Разработанное определение «фишинга» записывается в тетради и на доске.

Упражнение 2. «Продажа шоколада»

Ход занятия:

1) Из обучающихся выбирается два человека на роли «потенциальный клиент» и «продавец».

2) «Продавец» и «клиент» инструктируется по отдельности.

Роль клиента: Вы – владелец кафетерия на 21 этаже. Вы заходите в лифт и едете на работу.

Роль продавца: Вы встречаете в лифте перспективного потенциального клиента. Вы с ним знакомы заочно – знаете, что он владелец кафетерия на 21 этаже. У Вас есть около 30 секунд, чтобы убедить его купить у Вас партию нового шоколада. Задача продавца: Сделать хорошую самопрезентацию и за 30 секунд настолько заинтересовать собеседник разговором, чтобы он был готов дальше уделить свое внимание вам.

3) Разыгрывается ситуация.

Вопросы после упражнения: Какой результат достигнут? Что получилось/не получилось? Что можно было сделать лучше? Какие приемы убеждения использовались?

4) Обсуждается какие контрприемы можно использовать, чтобы отказаться от приобретения товара.

Лекция 4 «Поддельные товары, фейковые продажи, мошенничество в сети»

«Фейковый» постинг в сети

Социальные сети создают иллюзию живого общения, и информация, полученная из них, зачастую воспринимается как «сведения из первых рук» или «свидетельства очевидцев». В общественном сознании они часто противопоставляются традиционным СМИ, которые неизбежно ангажированы и предвзяты.

Интересный факт:

Никто точно не знает, сколько в сети ботов, а сколько – живых пользователей.

Однако существуют методы оценки трафика с различных IP-адресов, согласно которым до 60% заходов на интернет-страницы происходит в автоматическом режиме, без участия человека.

Интернет давно живет собственной жизнью: сетевые роботы создают страницы, имитируют их посещаемость, пишут и оценивают посты. Все ради накрутки просмотров и наращивания прибылей.

Однако, вспомним, что главной задачей социальных сетей является извлечение прибыли из рекламы и продаж. Первое, что для этого требуется, это технологии манипулирования мнением пользователей. Основой для такого манипулирования служат ложные или «фейковые» аккаунты, а также технологии автоматизированного постинга.

Наиболее примитивной технологией такого рода была уже устаревшая к настоящему времени **мимикрия**. В социаль-

ных сетях создавался аккаунт, личные данные и характеристики которого оптимально подходят для раскрутки у целевой аудитории, например, «успешная женщина» – для продажи тренингов личностного роста.

Далее постинг и общение велись уже от лица этого аккаунта, что позволяло легко завоевывать доверие людей. Используясь с коммерческими, а нередко и с мошенническими целями, эта технология показала высокую эффективность, в особенности в сфере адресных продаж. Ее существенным недостатком была высокая трудозатратность («фейковый» аккаунт все равно обслуживал один человек) и невозможность организации массового постинга.

Ситуацию изменили программные средства, позволявшие одному пользователю одновременно обслуживать несколько аккаунтов в различных соци-

альных сетях или интернет-форумах. Они получили общее название **мультиаккаунт** или **мультиакк**.

По сути, мультиакк представляет собой программный интерфейс, позволяющий одновременно поддерживать до нескольких десятков «фейковых» пользователей в режиме он-лайн. Один оператор управляет этими аккаунтами, публикует и комментирует посты, проставляет лайки и дизлайки и пр. Понятно, что у неподготовленного пользователя это создает иллюзию массовой поддержки (или критики) определенных товаров, людей или идей. Именно такие операторы и называются, в просторечии, профессиональными «сетевыми троллями».

Интернет, а в особенности социальные сети, служат дискуссионной площадкой, а для многих и вовсе единственной возможностью выразить свое мнение. Мультиакк позволил организовывать на практике технологию многоуровневого постинга. В ее рамках «фейковые» аккаунты одного или нескольких операторов спорят между собой, создавая впечатление широкой общественной дискуссии. В эту «дискуссию» организаторы вбрасывают целевой тезис, отстаивая его и выдавая за позицию большинства.

Нередко операторы организуют сложные схемы взаимодействия пользователей, к примеру:

Интересный факт:

По данным авторского исследования: 75% нижегородской молодежи не знают, что такое «мультиакк», а 11,1% – верят, что в онлайн-обсуждениях участвуют только реальные люди.

Схема взаимодействия операторов при организации «фейковой» дискуссии

Оператор I уровня:

- Знает целевой тезис, который нужно отстаивать.
- Поддерживает авторитетные, раскрученные аккаунты.
- Активно защищает целевой тезис.

Оператор II уровня:

- Не знает о целевом тезисе, но знает аккаунты I уровня.
- Использует свои аккаунты, для защиты и поддержки постов I уровня.
- Защищает целевой тезис опосредованно, не зная о нем.

Оператор III уровня:

- Знает целевой тезис, который нужно отстаивать.
- Использует свои аккаунты, чтобы спорить с тезисом, выражать сомнения, задавать вопросы.
- В итоге, его виртуальные аккаунты проигрывают спор, соглашаются с целевым тезисом.

У стороннего пользователя не возникает никаких сомнений, что он видит сообщество, активно обсуждающее проблему и приходящее к верным выводам. Группы операторов, действующие вместе по единой схеме на интернет-сленге называются «фабриками троллей».

Впрочем, на практике такие сложные схемы используются редко, в особо важных случаях. Гораздо чаще «интернет-тролли» просто постят сотни одинаковых сообщений от лица разных аккаунтов, формируя видимость массовой поддержки целевого тезиса.

Интерактивное задание к лекции «Поддельные товары, фейковые продажи, мошенничество в сети»

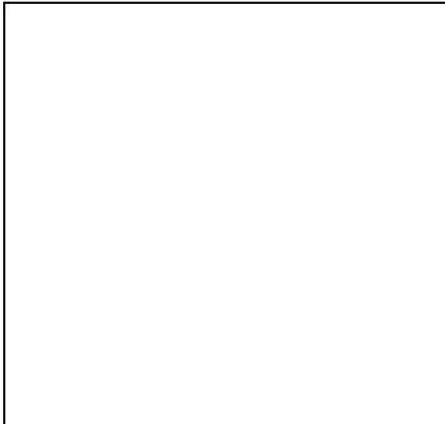
Цель занятия – сформировать у обучающихся систему представлений о фейковых продажах и мошенничестве в сети, а также навыки противостояния им.

Ход занятия:

1. Занятие проводится в стиле бортового журнала.

Преподаватель читает лекцию «Поддельные товары, фейковые продажи, мошенничество в сети», а обучающиеся отражают материалы в бортовом журнале.

В занятии используется упрощенная система бортового журнала.

БОРТОВОЙ ЖУРНАЛ	
ИМЯ _____	ТЕМА _____
ДАТА _____	ВРЕМЯ РАБОТЫ _____
КЛЮЧЕВЫЕ ПОНЯТИЯ СООБЩЕНИЯ	РИСУНОК (СХЕМА)
_____	

Полная схема бортового журнала:

*Burke K. Midful School: Yow to assess authentic learning.
Revised edition. IL: IRI/SkyLight Training and Publishing, Inc. 1994. - P.85.*

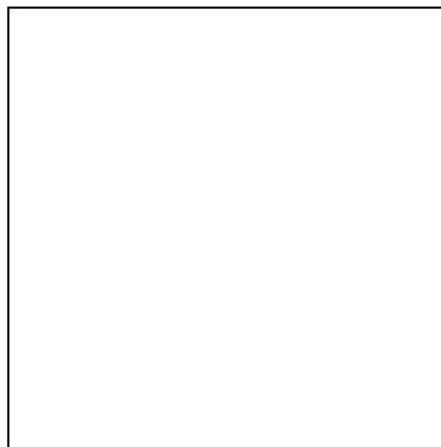
БОРТОВОЙ ЖУРНАЛ

ИМЯ _____ ТЕМА _____

ДАТА _____ ВРЕМЯ РАБОТЫ _____

КЛЮЧЕВЫЕ ПОНЯТИЯ СООБЩЕНИЯ

РИСУНОК (СХЕМА)



СВЯЗИ, КОТОРЫЕ Я МОГУ УСТАНОВИТЬ:

ОСТАВШИЕСЯ ВОПРОСЫ:

ПОЛНОТА ОТОБРАЖЕНИЯ ОСНОВНЫХ ПОНЯТИЙ _____
УЧАСТИЕ В ГРУППОВОЙ ДИСКУССИИ _____
ЦЕННЫЕ ИДЕИ, ПРЕДЛОЖЕНИЯ _____
СХЕМА СООБЩЕНИЯ _____
СУММА: _____

Далее обучающиеся фиксируют подзаголовок каждого нового раздела лекции и фиксируют то, что рассказал преподаватель.

Фиксировать можно в виде схем, графиком, таблицами или просто текста.

Возможные разделы лекции:

- Виды фейковых продаж;
- Противодействие фейковым продажам;
- Признаки мошенничества в сети;
- Виды мошенничества в сети;
- Способы противодействия мошенничества в сети.

После того, как преподаватель прочтет всю лекцию, а студенты все графически зафиксируют в бортовом журнале, заполняется раздел «Ключевые слова».

2. Обсуждаются заполненные бортовые журналы.

Каждый студент демонстрирует свой журнал, объясняет, какую информацию он счел важным отразить.

По итогам обсуждения выбирается лучший журнал, наиболее точно и подробно отражающий содержание лекции.

Преподаватель корректирует или дополняет усвоенную студентами информацию, снимает противоречия, если они возникают.

Копии лучшего журнала раздаются всем участникам группы.

5. Учебно-методическое обеспечение занятий семинарского типа

Семинар 1 «Киберзависимость, вовлечение в сообщества»

Тренинг «Профилактика киберзависимости»

Цель тренинга – привлечь внимание подростков к проблемам, связанным с киберзависимостью и выявлением склонности к ней.

Задачи:

1. Повысить уровень информированности обучающихся о киберзависимости;

2. Повысить уровень критического мышления по оценке своего собственного поведения в сети Интернет и особенностей использования мобильных гаджетов;

3. Мотивировать к дальнейшему самостоятельному развитию навыков безопасного, ответственного, осознанного использования сети Интернет.

План тренинга:

1. Введение. Принятие правил работы группы. (3 мин.)

2. Информационный блок. (15 мин.)

3. Приобретение практических навыков. (65 мин.)

4. Завершение работы. Оценка тренинга участниками группы (7 мин.)

План-конспект:

1. Введение. Принятие правил работы группы.

На этом этапе ведущие представляются и описывают цели и задачи тренинга. Ожидания участников можно выяснить в короткой беседе. Ведущий кратко объявляет правила работы и объясняет их значение.

2. Информационный блок.

Цель – дать обучающимся информацию об определении, признаках и видах киберзависимости.

Ведущий приводит результаты авторских исследований, представленных в пособии, в разделе текст лекций. Ведущий в форме вопросов проверяет мнение участников об актуальности обсуждаемой проблемы для них.

Методика проведения этого блока зависит от уровня информированности участников: если он низкий, то используем лекцию, если высокий – то беседу.

3. Приобретение практических навыков.

Цель этапа – осознание участниками важности ответственного отношения к своим собственным действиям в сети Интернет, а также развитие контроля за своим Интернет-потреблением.

Упражнение 1.

Цель: показать негативное влияние наркотиков на человека, семью и общество.

Работа осуществляется в малых группах

Ход работы:

1) Группа делится на малые группы.
2) Каждой группе участников необходимо записать на листах бумаги ответы на следующие вопросы:

1-я группа: Какие проблемы возникают у человека, который попал в зависимость от Интернета?

2-я группа: Какие проблемы возникают у семьи Интернет-зависимого?

3-я группа: Какие проблемы возникают у друзей (окружения) Интернет-зависимого?

4-я группа: Какие проблемы возникают в школе, где есть наркозависимые?

5-я группа: Какие проблемы возникают в районе или городе, где много Интернет-зависимых?

3) Группы зачитают свои ответы. Все бумаги с ответами склеиваются, чтобы получить единое поле проблем, возникающих по вине киберзависимости.

4) После того, как группы зачитают свои ответы, участникам предлагается ответить на вопрос: кого больше всего задевает киберзависимость?

5) Обсуждение результатов выполнения упражнения.

Задача ведущего: привести группу к выводу: киберзависимость тяжело влияет не только на самого зависимого, ломая его здоровье и жизнь, но бьет и по его близким и, в конечном счете, по согражданам, государству.

Упражнение 2.

Цель: формирование у участников представлений о негативном влиянии киберзависимости на здоровье.

Ход работы:

1) Группа делится на малые группы.

2) Каждой группе участников ведущий по листу с изображением силуэта человека и предлагает в течение следующих 10 минут нарисовать или написать на силуэте негативные последствия киберзависимости для различных систем и органов организма человека.

3) Спустя 10 минут малые группы по очереди представляют свои наработки остальным участникам.

4) Обсуждение результатов выполнения упражнения.

Задача ведущего: показать участникам занятия, что киберзависимость может стать дорогой к инвалидизации человека.

Упражнение 3.

Цель: отработать навыки уверенного поведения, аргументированного отказа в ситуации выбора.

Ход работы:

1) Группа делится на малые группы. Каждой подгруппе предлагается одна из ситуаций:

– одноклассница убеждает зарегистрироваться в приложении для знакомств, а вы не доверяете знакомствам в Интернет;

– одноклассник (сосед, лидер двора) просит присоединиться к его команде в Интернет-соревновании, поскольку без еще одного игрока их дисквалифицируют, но игра может длиться от 3 до 5 часов;

– одноклассник (сосед, лидер двора) просит солгать его родителям, что вы вместе учите уроки, а сам будет участвовать в Интернет-игре у Вас дома, так как у себя дома родители ему играть запретят.

2) Малым группам предлагается в течение 7 минут придумать как можно больше аргументов для отказа в этой ситуации.

3) После подготовки каждая подгруппа «проигрывает» свою ситуацию перед остальными участниками. Один играет роль «уговаривающего», другой – «отказывающегося».

4) Ведущий предлагает использовать в каждой ситуации 3 стиля отказа: уверенный, агрессивный и неуверенный. Каждый стиль демонстрирует только один участник.

Если ведущий чувствует, что роль уговаривающего может быть исполнена участниками недостаточно хорошо, он может сыграть ее сам.

5) Далее следует обсуждение необходимости приобретения навыков «отказа», отстаивания своей точки зрения, аргументирования своей позиции, влияния тех или иных форм отказа на дальнейшие отношения. Дискутируется вопрос о сложностях и преимуществах ответственного поведения.

Упражнение 4.

Цель: выработать несколько различных стратегий поведения, которые позволяют не вступать в созависимые отношения с зависимыми от Интернет-игр; дают возможность сохранить личную безопасность и в то же время помочь близкому человеку.

Ход работы:

1) Ведущий предлагает группе обсудить вопрос «Как следует строить отношения с другом, злоупотребляющим гаджетами и компьютерными играми?». Участники высказывают свои идеи и мысли на заданную тему.

2) Ведущий направляет ход обсуждения, выявляет нелогичные и дискриминационные моменты, уточняет правильность понимания группой отдельных высказываний.

3) Дискуссия заканчивается, когда у группы складывается единая стратегия помощи другу с зависимостью от Интернет-игр.

4. Завершение работы. Оценка тренинга участниками группы.

На этом этапе ведущий выясняет у участников, что понравилось, или что не понравилось в ходе тренинга, оправдались ли их ожидания и подводит итоги проведенной работы. Если есть время, можно провести упражнение «Ощущения»: ведущий просит каждого участника сказать, какие чувства у них вызвало это занятие. Также ведущий собирает информацию о темах, связанных с киберугрозами, которые обучающиеся хотели бы изучить отдельно.

Семинар 2 «Кибербуллинг и интернет-обусловленное поведение»

Тренинг «Скажи травле – «нет!»»

Цель тренинга – привлечь внимание подростков к проблемам, связанным с буллингом в сети Интернет.

Задачи:

1. Повысить уровень информированности обучающихся о проблеме выявления буллинга и безопасного поведения в сети Интернет;
2. Повысить уровень критического мышления по оценке своего собственного поведения в сети Интернет;
3. Мотивировать к дальнейшему самостоятельному поиску информации о противодействии буллингу.

План тренинга:

1. Введение. Принятие правил работы группы. (3 мин.)
2. Оценка уровня информированности группы. (10 мин.)
3. Актуализация проблемы. (7 мин.)
4. Информационный блок. (15 мин.)
5. Приобретение практических навыков. (45 мин.)
6. Завершение работы. Оценка тренинга участниками группы (10 мин.)

План-конспект:

1. Введение. Принятие правил работы группы.

На этом этапе ведущие представляются и описывают цели и задачи тренинга. Ожидания участников можно выяснить в короткой беседе. Ведущий кратко объявляет правила работы и объясняет их значение.

2. Оценка уровня информированности группы.

Этот этап может быть проведен в форме беседы, в процессе которой ведущий, при помощи последовательных вопросов выясняет уровень информированности.

Важно создать такую атмосферу, в которой члены группы будут свободно высказываться, не бояться ошибиться, не бояться осуждения. Роль ведущего заключается в дополнении, уточнении и коррекции ошибочных представлений.

3. Актуализация проблемы.

Ведущий приводит результаты авторских исследований, представленных в пособии, в разделе текст лекций. Ведущий в форме вопросов проверяет мнение участников об актуальности обсуждаемой проблемы для них.

4. Информационный блок.

Цель – дать обучающимся информацию о том, какие действия можно квалифицировать как кибербуллинг; какие виды кибербуллинга существуют; как узнать киберагрессора; как не стать кибержертвой; как правильно общаться в социальных сетях; как выбирать собеседников в социальных сетях; что делать, если уже столкнулся с кибертравлей.

Методика проведения этого блока зависит от уровня информированности участников: если он низкий, то используем лекцию, если высокий – то беседу.

5. Приобретение практических навыков.

Цель этапа – осознание участниками важности ответственного отношения к своим собственным действиям в сети Интернет, а также развитие навыков уверенного поведения и аргументированного отказа в ситуации выбора.

Упражнение 1.

Ход работы:

1) Выбирается доброволец «на главную роль». При желании ведущий может выполнять эту роль самостоятельно. Ведущий предлагает ему разыграть следующую роль: участник должен убедить одноклассника выложить в Интернет ненадлежащее фото одноклассницы, сделанное на одной из школьных вечеринок. Участник может самостоятельно выбирать любые способы убеждения и объяснения мотивов своих действий.

2) Выбираются еще три участника. Им будет предложено отказываться от чего-либо: первому игроку – агрессивно, второму участнику – уверенно, третьему – не уверенно.

3) Разыгрываются сценки.

4) После разыгрывания ситуаций, происходит обсуждение:

- Как чувствовал себя человек в ситуации давления?
- Какой вариант отказа оказался более эффективным (мнение группы и главного героя)?
- Что можно было сделать, чтобы отказ был более убедительным?
- Какие аргументы использовались для убеждения?
- Как чувствовали себя основные участники в сценке и участники группы?

Упражнение 2.

Цель: игра позволяет участникам лучше узнать друг друга, позволяет почувствовать себя на месте другого человека, способствует росту сплоченности группы.

Задача ведущего – помочь участникам осознать, что внешность, манера поведения и общения может создать обманчивое впечатление о личности, что порой мы склонны делать скоропалительные выводы о человеке без достаточных оснований, опираясь на собственные стереотипы.

Ход работы:

1) Участникам предлагается разбиться на пары. Желательно, чтобы партнеры были наименее знакомы друг другу.

2) В течение 10 минут партнерам предлагается выяснить друг у друга интересы, привычки, увлечения и другие личные особенности.

3) После этого участники садятся в круг. Один человек сидит на стуле, его партнер стоит у него за спиной.

4) Все члены группы задают вопросы, обращаясь последовательно к каждому из сидящих. От его имени дает ответ человек, который стоит за спиной. Сидящий не комментирует правильность или неправильность ответов.

5) После того как каждому было задано 2-4 вопроса, участники меняются местами. Процедура повторяется.

6) В конце игры участники делятся своими чувствами. Обсуждение происходит по схеме:

– Насколько правильными были ответы, которые давал за вас партнер?

– Какие чувства вы испытывали, когда за вас отвечал другой человек?

– Трудно было отвечать за другого?

– Сравнивали вы увлечения другого человека со своими?

7) Ведущий подводит итоги, делая акцент на следующих выводах: «все люди разные»; «первое впечатление о человеке может быть ложным»; «внешность, манера поведения и общения может создать обманчивое впечатление о личности», «для того чтобы составить мнение о человеке, одной беседы с ним недостаточно»; «порой люди делают выводы скоропалительно, без достаточных оснований».

6. Завершение работы. Оценка тренинга участниками группы.

На этом этапе ведущий выясняет у участников, что понравилось, или что не понравилось в ходе тренинга, оправдались ли их ожидания и подводит итоги проведенной работы. Если есть время, можно провести упражнение «Ощущения»: ведущий просит каждого участника сказать, какие чувства у них вызвало это занятие. Также ведущий собирает информацию о темах, связанных с киберугрозами, которые обучающиеся хотели бы изучить отдельно.¹⁹

¹⁹ Я хочу провести тренинг: пособие для начинающего тренера, работающего в области профилактики ВИЧ/СПИД, наркозависимости и инфекций, передающихся половым путем. 3-е изд. / Яшина Е., Степанова О., Камалдинов Д. и др. – Новосибирск, 2005. – 211 с.

Деловая игра «Фишинг данных»

Цель игры: отработка учащимися навыков и приемов интернет-дискуссий, выработка навыков критического восприятия информации, умения противостоять технологиям фишинга данных, развитие сетевой грамотности.

Деловая игра проводится в группах учащихся от 8 человек. Для эффективной работы участникам требуются электронные (десктопные или мобильные) устройства с выходом в интернет и общим чатом (Viber, Telegramm или другой подобный мессенджер). Игра может проводиться он-лайн, полностью в удаленном режиме. В отсутствии электронных устройств можно пользоваться ручными записями, но это снижает эффективность работы.

Игровой процесс:

Суть игры заключается в попытках одних участников в процессе не принужденного общения получить «личные данные» других. Роль «личных данных» в игре может исполнять любая редкая информация, но предпочтение следует отдавать тому, что банки обычно используют как кодовое слово: девичья фамилия матери, имя питомца, любимый цвет и пр.

Все участники игры получают карточки-задания. Карточки вручаются анонимно и определяют позицию, которую участники должны занять в ходе дискуссии. Организатор может прописать в них различные начальные условия, однако лучше всего ввести карточки следующих типов:

- «Мошенник». Его цель – собрать максимальное количество данных пользователей. Он охотится не за всеми данными, а только за тремя известными ему типами. Мошенников должно быть несколько, они должны знать друг друга и заранее разработать план добычи данных. В группе не должно быть более 20% «мошенников».
- «Пользователь». Свободно общается в чате, пытаясь оберегать свои «личные данные». Получает обширный список данных, которые нужно сообщить другим пользователям и не знает, за чем конкретно охотятся мошенники и сколько их. Большинство обучающихся должны стать «пользователями».

Примеры карточек:

Карточка «Пользователь»

Вы – обычный интернет-пользователь. Общаетесь в группе, которую посещаете уже давно. Кажется, сегодня здесь что-то интересное. Надо поучаствовать в обсуждении и в процессе обязательно сообщить другим участникам:

1. Размер ноги.
2. Диагональ экрана мобильного.
3. Любимый цвет.
4. Любимая марка авто.
5. Любимая газировка.
6. Любимый салат.
7.

Но ничего другого.

Здесь должно быть 20-30 позиций. Это необходимо, чтобы запутать «пользователя», спровоцировать его неконтролируемо сообщать любую информацию.

Карточка «Мошенник»

Вы – мошенник, который охотится за персональными данными пользователей. Вам необходимо собрать информацию как можно быстрее. Можно использовать любые приемы для получения информации.

Вас интересует:

1. Девичья фамилия матери.
2. Имя питомца.
3. Объем оперативной памяти телефона.

Всего 3 позиции, которых нет в списке пользователя. Расчет здесь на то, что делаясь всем подряд из своего списка, пользователь не заметит трех дополнительных вопросов.

Получив карточки, обучающиеся начинают общение в чате. Преподаватель наблюдает за попытками «мошенников» добыть «личные данные». Необходимо оценивать:

1. Аргументацию позиций участников.
2. Использование участниками специфических полемических приемов.

3. Способность объединяться с единомышленниками и сотрудничать.
4. Способность противостоять попыткам манипуляции.
5. Психологическую устойчивость и способность сохранить душевное равновесие в споре.

По итогам обсуждения организатор может создать в чате голосование по теме дискуссии. Оно должно четко разделять позиции сторон. К примеру:

Кому можно предоставлять свои персональные данные:

1. Никому нельзя. В исключительных случаях только при очном визите под роспись.
2. Можно на официальных сайтах магазинов, учреждений, на ресурсах, которые шифруются HTTPS
3. Все наши данные уже всем известны, неважно, кто спрашивает их сейчас.

По завершению дискуссии преподавателю необходимо обсудить с обучающимися ее особенности и результаты. Следует уточнить:

У «мошенников»:

- была ли у них стратегия и как она менялась в процессе развития дискуссии;
- какие приемы они использовали и как;
- какие из них оказались наиболее эффективными;
- к чему оказалась восприимчива/невосприимчива аудитория;

У «пользователей»:

- поняли ли они, кто является мошенником;
- удалось ли им распознать использовавшиеся приемы манипуляции;
- каково быть объектом/субъектом манипуляции;
- легко ли сохранить самообладание в дискуссии;

Преподаватель оценивает участие каждого в дискуссии с точки зрения активности, аргументации, способности противостоять манипулятивному воздействию.

Аналитическая справка «Оценка подлинности сайта»

Цель работы: Провести экспертизу интернет-сайта и сделать предположение о его подлинности.

Работа выполняется в форме аналитической справки. В ходе ее подготовки обучающиеся должны следовать определенному алгоритму работы, который отражается в структуре документа. Это алгоритм и, соответственно, структура документа, должна выглядеть так:

I. Общая оценка сайта.

1. Доменная зона: общая характеристика.
2. Возраст сайта.
3. Дата регистрации.
4. Контент на сайте: анализ оригинальности.

II. Отзывы в сети и контакты

1. Отзывы на сайт и организацию.
2. Отзывы в справочниках и по номеру телефона.
3. Размещение в картах по адресу.

III. Оплата, скидки и доставка.

1. Тип оплаты.
2. Размер скидок.
3. Формы доставки.

IV. Проверка данных организации в сети.

1. Контакты.
2. Реквизиты.

V. Проверка кода сайта.

Просмотр кода (Cntr + U). Здесь сайты, содержащие ворованные элементы, будут иметь в коде следующие включения:

- (i)frame с чужим доменным именем;
- tppabs в любом виде;
- (a_)href с чужим доменным именем;
- document saved from в любом виде;
- mirrored с чужим доменным именем.

VI. Вывод о степени подлинности сайта.

Справка оформляется в электронном виде, в формате docx. Разделы I.1., I.2. и V необходимо снабдить скриншотами, отражающими содержательную часть анализа. Объем – не более 3 стр.

В ходе проверки работы преподаватель оценивает: грамотность, корректность и полноту анализа, структурирование данных, обоснованность вывода.

Семинар 4 «Поддельные товары, фейковые продажи, мошенничество в сети»

Деловая игра «Рынок фейков»

Цель игры: отработка учащимися навыков и приемов интернет-дискуссий, выработка навыков критического восприятия информации, умения распознавать фейковые продажи, развитие сетевой грамотности.

Деловая игра проводится в группах учащихся от 8 человек. Для эффективной работы участникам требуются электронные (десктопные или мобильные) устройства с выходом в интернет и общим чатом (Viber, Telegramm или

другой подобный мессенджер). Игра может проводиться он-лайн, полностью в удаленном режиме. В отсутствии электронных устройств можно пользоваться ручными записями, но это снижает эффективность работы.

Игровой процесс:

Суть игры заключается в общении учащихся между собой по вопросу приобретения поддельных товаров в сети. Типы товаров и прописанные в карточках участников роли заранее определяются организаторами. Это должен быть востребованный на данный момент товар (поп-ит, блютуз колонка, копии популярных кроссовок и т.п.) или услуга (психологический коучинг, тренинг личностного роста и т.п.).

Для дополнительного стимулирования участников можно использовать закрытые коробки с изображением или логотипом товара. Внутри можно поместить конфеты (включая «фейковые» - просто завернутые в фантик бумажки). В качестве платежного средства участникам можно выдать билеты банка приколов или подобные игровые деньги.

Далее ход игры описан на примере темы «Покупка – продажа кроссовок NIKE JORDAN» <https://nike-air-jordan1.com/muzhskie-nike-air-jordan>

В начале игры все участники получают карточки-задания. Карточки вручаются анонимно и определяют позицию, которую участники должны занять в ходе дискуссии. Организатор может прописать в них различные начальные условия, однако лучше всего ввести карточки следующих типов:

- «Продавец фейка». Обязан защищать свой магазин. Его цель – продать свой товар или услугу наибольшему количеству пользователей. Имеет смысл создать несколько «продавцов фейков», придерживающихся разных стратегий. К примеру, один уверяет, что его товар – оригинальный, второй – не скрывает, что это подделка и подчеркивает низкую цену. Эту карточку лучше вручать наиболее активным и коммуникабельным обещающим. В группе не должно быть более 20% «продавцов фейков».

- «Любитель фейков». Имеет опыт покупки фейковых товаров и не видит в этом ничего страшного. В группе не должно быть более 10% «любителей фейков».

- «Сомневающийся пользователь». Не доверяет фейковым продажам и опасается их. Пытается убедить аудиторию не связываться с подделками. В группе не должно быть более 10% «сомневающихся пользователей».

- «Пользователь». Эта карточка дает участнику свободу выбора и выражения позиции. Именно на мнение «пользователей» и пытаются влиять остальные. Большинство обучающихся должны стать «пользователями».

Пример карточек:

Карточка «Пользователь»

Вы – обычный интернет-пользователь. Во время обычного серфинга Вы наткнулись на сайт, где продают кроссовки, о которых вы уже давно мечтали.

Вы бы их купили, но сайт вызывает несколько вопросов. Вы решили задать их в чате.

Карточка «Любитель фейков»

Вы – обычный интернет-пользователь. Во время обычного серфинга Вы наткнулись на сайт, где продают кроссовки, о которых вы уже давно мечтали.

Вы хотите их купить и уже ввели данные своей банковской карточки. Даже предоплата вас не смущает, ведь вы уже несколько раз покупали брендовые товары по цене 1999 рублей.

Карточка «Сомневающийся пользователь»

Вы – обычный интернет-пользователь. Во время обычного серфинга Вы наткнулись на сайт, где продают кроссовки, о которых вы уже давно мечтали.

Вы хотите их купить, но в прошлом месяце, на таком же сайте, Вы заказали сумку PRADA, но прислали вам авоську за 200 рублей.

Карточка «Продавец фейка»

Вы – владелец фейкового бизнеса. Во что бы то ни стало вам нужно убедить пользователей, что ваш магазин имеет кристальную репутацию, а кроссовки шил сам Майкл.

Получив карточки, обучающиеся начинают общение в чате. Преподаватель наблюдает за попытками продавцов фейков склонить аудиторию на свою сторону и за реакцией.

Необходимо оценивать:

1. Аргументацию позиций участников.
2. Использование участниками специфических полемических приемов.
3. Способность объединяться с единомышленниками и сотрудничать.
4. Способность противостоять попыткам манипуляции.
5. Психологическую устойчивость и способность сохранить душевное равновесие в споре.

По итогам обсуждения преподаватель может создать в чате опрос. К примеру:

Приемлемо ли, на ваш взгляд, продавать подделки?

1. Продавать поддельные товары неприемлемо, на рынке могут быть только оригиналы.
2. Я не против подделок, но сам никогда их не куплю.
3. С удовольствием куплю поддельный товар, если будет хорошая скидка.
4. Магазины оригиналов и «фейков» должны быть четко разделены, чтобы покупатель всегда знал, за что платит.

По завершению дискуссии преподавателю необходимо обсудить с обучающимися ее особенности и результаты. Следует уточнить:

У «продавцов фейков»:

- была ли у них стратегия и как она менялась в процессе развития дискуссии;

- какие приемы они использовали и как;
- какие из них оказались наиболее эффективными;
- к чему оказалась восприимчива/невосприимчива аудитория;

У «пользователей»:

- изменили ли они свое изначальное мнение и почему;
- каково быть объектом/субъектом манипуляции;
- легко ли сохранить самообладание в дискуссии;
- управляемо ли общественное мнение;
- удалось ли им распознать использовавшиеся приемы манипуляции.

Преподаватель оценивает участие каждого в дискуссии с точки зрения активности, аргументации, способности противостоять манипулятивному воздействию.

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

Курс разработан с учетом необходимости развития у обучающихся практических навыков обеспечения собственной кибербезопасности, поэтому сочетает элементы классического обучения – лекции, и практического – занятия с составляющими тренинга. При этом значимое место в планировании курса имеет организация самостоятельной работы обучающихся. Самостоятельная работа – это планируемая учебная, учебно-исследовательская, научно-исследовательская работа обучающихся, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя.

Организация самостоятельной работы обучающихся позволяет создать условия, при которых они:

- самостоятельно приобретают недостающие знания из разных источников;
- учатся пользоваться приобретенными знаниями для решения познавательных и практических задач;
- приобретают и развивают коммуникативные умения (осуществляется во время активной индивидуальной работы на занятии, презентации выполненных заданий, данных преподавателем);
- развивают исследовательские умения (умения выявления проблем, сбора информации, наблюдения, проведения эксперимента, анализа, построения гипотез, обобщения);
- развивают системное мышление.

На всех этапах выполнения работы преподаватель оказывает консультативную помощь и методическое обеспечение.

Задания для самостоятельной работы обучающихся

Занятие «Киберзависимость, вовлечение в сообщества»

Задание – опросить 10 человек по мини-анкете о киберзависимости. Анкета предоставляется обучающемуся преподавателям и содержит такие вопросы, как:

Как часто Вы ощущаете раздражительность и беспокойство при отсутствии возможности посетить свой профиль в социальных сетях?

- часто
- иногда
- редко
- никогда
- затрудняюсь ответить

Насколько часто вы остаетесь online дольше, чем намеревались?

- всегда
- достаточно часто

- иногда
- редко
- никогда
- затрудняюсь ответить

Как часто Вы используете социальные сети, чтобы уйти от личных проблем?

- часто
- иногда
- редко
- никогда
- затрудняюсь ответить

Как вы считаете, существует ли психологическая болезнь – зависимость от Интернета?

- да
- нет
- затрудняюсь ответить

Результаты опроса обсуждаются с преподавателем на занятии. В ходе обсуждения обучающиеся смогут на основе личного опыта оценить масштабы распространения проблемы киберзависимости.

Занятие «Кибербуллинг и интернет-обусловленное поведение»

Задание – заполнить таблицу.

Характерные черты поведения	
киберагрессора	жертвы кибербуллинга

Заполненные таблицы обсуждаются с преподавателем на занятии. В ходе обсуждения обучающиеся смогут анализировать поведения окружающих с точки зрения угрозы кибербуллинга, а также критически оценить собственное поведение в сети Интернет.

Занятие «Фишинг данных, навязывание товаров/услуг»

Задание – привести три примера фишинга данных, с которыми пришлось столкнуться обучающемуся или его окружения, а также описать способы защиты.

Например: Буквально несколько дней назад мой аккаунт в сети «ВКонтакте» был взломан. Те, кто это сделали, тут же разослали моим друзьям (а их у меня больше 800 человек) сообщения-приветы. А потом, тем, кто ответил пришла просьба одолжить денег до субботы, номер карты, куда сбрасывать

средства и обещание отдать долг. Как только я увидела эти сообщения, то срочно меняла пароли.

Данное упражнение позволит собрать большой объем практических кейсов по теме фишинга. Обучающиеся смогут продемонстрировать свой успешный опыт борьбы с кражей идентификационных данных, что, с одной стороны, повысит их уверенность в собственных навыках обеспечения кибербезопасности, а, с другой, позволит на чужом опыте изучить возможные киберугрозы.

*Занятие «Поддельные товары, фейковые продажи,
мошенничество в сети»*

Задание – обучающимся предлагается написать два честных отзыва о товаре на сайтах в сети Интернет. Цель – с одной стороны, узнать насколько легко или сложно оставлять отзывы в сети Интернет, с другой стороны, сформировать навыки критической оценки достоверности или недостоверности отзывов.

7. Фонды оценочных средств для аттестации по дисциплине

Текущий контроль успеваемости проходит в форме тестирования.

Тест

Инструкция: На выполнение теста дается 15 минут. В каждом вопросе необходимо выбрать один правильный ответ из предложенных.

1. Стремление человека к уходу от реальности путем искусственного изменения своего сознания посредством веществ или фиксации внимания на определённых видах деятельности – это:

- a. аддикция
- b. девиация
- c. деструкция
- d. синдром

2. Гемблер – это человек, страдающий зависимостью от:

- a. азартных ставок в Интернете
- b. покупок в Интернете
- c. игр в Интернете
- d. знакомств в Интернете

3. Ключевым признаком киберзависимости является:

- a. бесцельное потребление информации в сети Интернет
- b. неспособность контролировать время в сети Интернет
- c. отсутствие друзей вне сети Интернет
- d. чрезмерная трата денег в сети Интернет

4. Популярность киберобщения в сети Интернет объясняется:
- активностью и популярностью собеседников
 - анонимностью и дистанцированностью собеседников
 - креативностью и скрытностью собеседников
 - открытостью и грамотностью собеседников
5. Информационная шумиха, внезапная популярность, возникающая вокруг события или некой тематики называется:
- бренд
 - патент
 - тренд
 - хайп
6. Кибербуллинг всегда подразумевает
- намеренный и неоднократный вред
 - периодический и эмоциональный вред
 - умышленный и длительный вред
 - физический и экономический вред
7. Киберагрессор – это человек, который
- наносит ущерб
 - наблюдает за травлей
 - поддерживает травлю
 - страдает от травли
8. Троллинг – это
- обмен оскорбительными сообщениями в сети
 - преследование пользователя в сети
 - рассылка унижительной информации в сети
 - социальная провокация пользователя в сети
9. Попытка выяснить данные банковской карты другого пользователя называется:
- дейтинг
 - диссинг
 - фишинг
 - фрэпинг
10. Информационная мистификация или намеренное распространение дезинформации в социальных медиа с целью введения в заблуждение, для того чтобы получить запланированную выгоду – это
- дизлайк
 - пранк
 - фейк
 - хайп

Промежуточный контроль успеваемости проходит в форме защиты проекта.

Проект

Задание: разработка проекта по снижению влияния киберугроз на общественные отношения.

Цель создания проекта – привлечение внимание к решению актуальной социальной проблемы – рост числа киберугроз в сети Интернет, и количества Интернет-мошенничеств.

Требования к содержанию проекта:

Готовый социальный проект должен содержать следующие обязательные блоки²⁰:

<i>Название проекта</i>	<i>Выбирается обучающимся самостоятельно</i>
Актуальность проекта	Описывается проблема, которая должна решаться с помощью разрабатываемого проекта. Обосновывается её значимость.
Адресность (целевая аудитория проекта)	На кого нацелен ваш проект? Подробно опишите целевую аудиторию вашего проекта.
Цель и задачи проекта	Какие цель (одна) и задачи (несколько) вы ставите перед собой при реализации проекта? Цель – это описание предполагаемого результата, которого планируется достичь в результате работы.
Сроки реализации проекта	В течение какого периода времени вы будете реализовывать ваш проект? Можно ли его повторять ежегодно?
Содержание и план проекта	Что будете делать для реализации цели? В чем заключается суть проекта? Какова последовательность ваших действий при подготовке и реализации проекта? Представьте план-график реализации проекта.
Новизна проекта	Какой опыт по решению заявленной вами проблемы уже есть в зарубежной практике? В российской практике? В чем новизна предложенного вами проекта? Что особенного в Вашем проекте, что Вы взяли и что модернизировали?
Риски проекта и их профилактика	С какими рисками вы можете столкнуться при реализации проекта? Предложите возможные пути их предотвращения или смягчения.

²⁰ Мигунова А.В. Социальный проект «Прыж'ок» / А.В. Мигунова, Д.А. Кормщиков, Е.В. Милкина, Г.С. Пусяк // Надежды: Сборник научных статей студентов / Научный редактор З.Х. Саралиева. – Вып. 6. – Н. Новгород: Изд-во НИСОЦ, 2011. – С. 64-70.

Ресурсное обеспечение проекта	Какие ресурсы необходимо вам привлечь для реализации проекта (укажите виды ресурсов и расшифруйте потребности)?
Бюджет проекта	Представьте примерную смету расходов, указав на что именно требуются средства, а что можно сделать бесплатно.
Управление проектом	Представьте схему управления проектом.
Оценка эффективности проекта	На основании каких критериев вы сможете судить, что достигли желаемого результата?

Проект представляется в форме презентации. Объем презентации не менее 10 слайдов.

Подведение итогов осуществляется с учётом следующих критериев оценки:

- 1) актуальность;
- 2) оригинальность текста и подачи;
- 3) аргументированность и глубина раскрытия содержания темы;
- 5) креативность, новизна идеи;
- 6) точность и доходчивость языка и стиля изложения;
- 7) соблюдение временного регламента.

Критерии оценивания устной презентации проекта

	<i>Качество самостоятельной подготовки</i>	<i>Содержание ответа</i>	<i>Полнота отражения информации</i>	<i>Выступление и умение отвечать на вопросы</i>
за-чтено	При подготовке к ответу обучающимся проведено качественное теоретическое исследование по теме, с использованием списка предложенной литературы.	Содержание проделанной работы раскрыто в полном объеме.	Текст ответа содержит не только данные анализа, но и представлена точка зрения обучающегося.	Владение культурой речи, согласованность устного выступления, аргументированное представление и защита собственного аналитического материала. Обучающийся уверенно владеет материалом и быстро правильно отвечает на вопросы, задаваемые преподавателем.

не за- чено	При подготовке к ответу обучающегося не проведено теоретическое исследование, представленный материал носит излишне обобщенный, описательный характер.	Основное содержание проделанной работы раскрыто не полно, возможно по причине того, что сама подготовка к устному опросу проведена некачественно, не изучена дополнительная литература. Путаница в изложении материала.	При ответе обучающийся ограничивается знаками, полученными на занятии, не может аргументированно представить свою точку зрения или привести пример.	Речь недостаточно грамотная, содержит содержательные и логические ошибки, недостаточно аргументированное представление и защита материала. Обучающийся не уверенно владеет материалом, поэтому не может ответить на вопросы преподавателя, или ему требуется несколько дополнительных наводящих вопросов.
----------------	--	--	---	--

8. Учебно-методическое и информационное обеспечение курса

Основная литература

1. Авазов К.Х. Влияние интернет-зависимости на личность подростка // Актуальные проблемы гуманитарных и естественных наук. – 2016. – № 4-6. – С. 71-74.
2. Агеева Н.А. Особенности Интернет-зависимых личностей / Н.А. Агеева // Вестник Российского университета дружбы народов. – 2007. – № 1. – С. 70-79.
3. Алексеев А.С. Фишинг: интернет-мошенничество с применением социальной инженерии / А.С. Алексеев // Вестник современных исследований. – 2019. – № 1.13(28). – С. 12-16.
4. Апатова Н.В. Особенности поведения потребителей в интернет / Н.В. Апатова // Вестник Тверского государственного университета. Серия: Экономика и управление. – 2020. – № 3(51). – С. 19-29. – DOI 10.26456/2219-1453/2020.3.019.
5. Бенькова В.Ю., Бенькова О.А. Особенности межличностных отношений подростков, склонных к Интернет-зависимости // Наука, Образование и Инновации: сборник статей Международной научно-практической конференции. – Уфа: АЭТЕРНА, 2017. – С. 181-186.
6. Богданова О.А. Интернет-зависимость у детей и подростков / О.А. Богданова // Вестник МГПУ. – 2014. – №1(27). – С. 54-59.

7. Бойков А.Е. Первичная профилактика различных видов зависимостей детей и подростков в образовательной среде / А.Е. Бойков // Молодой ученый. – 2014. – №3. – С. 871-874.
8. Братусин А.Р. О значении профилактики буллинга, моббинга и кибербуллинга в контексте повышения уровня цифровой грамотности молодежи: педагогический аспект / А.Р. Братусин, С.А. Спесивцев, А.Ю. Расторгуев // Проблемы современного педагогического образования. – 2020. – № 67-4. – С. 55-58.
9. Варламова С. Интернет-зависимость молодежи мегаполисов: критерии и типология / С. Варламова, Е. Гончарова, И. Соколова // Мониторинг общественного мнения. Экономические и социальные перемены. – 2015. – № 2. – С. 165-181.
10. Васильева Ю.Е. К вопросу о проблеме интернет-зависимости в современном обществе / Ю.Е. Васильева, И.А. Ивашина, П.П. Попов, И.Г. Рыжов // Прикладные информационные аспекты медицины. – 2014. – Т. 17. – № 1. – С. 48-51. [Электронный ресурс] – URL: <https://www.elibrary.ru/item.asp?id=21357604>
11. Войскунский А.Е. Актуальные проблемы зависимости от интернета // Психологический журнал. – 2004. – Т. 25. № 1. – С. 90-100.
12. Гайнцев Е.Г. Анализ Интернет-зависимости и механизм её формирования // Российский электронный научный журнал. – 2014. – №5. – С. 54-61.
13. Галицына А. М. «Группы смерти» как средство манипулирования сознанием // Развитие общественных наук российскими студентами. – 2017. – №4. – С. 15-21.
14. Дюркгейм Э. Норма и патология. Социология преступности (Современные буржуазные теории). – М.: Прогресс, 1966. – С. 39–44.
15. Жихарева Л.В. Виртуальные группы смерти: методология исследования // Научные ведомости БелГУ. Серия: Гуманитарные науки. – 2018. – №1. – С. 12-18.
16. Замятина А.А. Подростковый алкоголизм как социально психологическая проблема / А.А. Замятина, Д.В. Каширский // NOVAINFO.RU. – 2015. – Т. 1. № 5. – С. 246-248.
17. Зинцова А. С. Социальная профилактика кибербуллинга // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия: Социальные науки. – 2014. – №. 3 (35).
18. Игдырова С.В., Чикляукова Е.В., Мукминов Р.Р. Социальная работа с подростками склонными к киберрадикации / С.В. Игдырова, Е.В. Чикляукова, Р.Р. Мукминов // Вестник Дмитровского гражданского инженерно-технологического института. – 2014. – № 1(3). – С.149-157.
19. Исакова И.А. Гаджетизация: эффекты влияния на общественные процессы / Т. Н. Захаркина, И. А. Исакова // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия: Социальные науки. – 2019. – № 3(55). – С. 115-121.

20. Исакова И.А. Интернет-зависимость как путь к инвалидизации подростков/ И.А. Исакова // Международная научно-практическая конференция «Инвалиды – Инвалидность – Инвалидизация». – 2018. – С. 601-604. Режим доступа: <http://www.fsn.unn.ru/wp-content/uploads/sites/5/Invalidy-27-28.09.2018.pdf> (дата обращения: 09.04.2019).
21. Исакова И.А. Информатизация и гаджетизация современного общества и детства / И.А. Исакова, А.Л. Янак // Цифровой ученый: лаборатория философа. – 2019. – Т. 2. – № 1. – С. 131-145. – DOI 10.5840/dspl20192114.
22. Итоговый отчет исследования «Дети России онлайн» [Электронный ресурс] // Официальный сайт проектов Фонда Развития Интернет. – URL: http://detionline.com/assets/files/helpline/Final_Report_05-29-11.pdf (дата обращения: 10.04.2019).
23. Кирюхина Д.В. Кибербуллинг среди молодых пользователей социальных сетей / Д.В. Кирюхина // Современная зарубежная психология. – 2019. – Т. 8. – № 3. – С. 53-59. – DOI 10.17759/jmfp.2019080306.
24. Королева Д.Е., Новичихина Е.В. Интернет-зависимость, компьютерная игромания – глобальная причина развития гиподинамии молодежи XXI века / Д.Е. Королева, Д.Е. Новичихина. – Барнаул: Изд-во: ФГБОУ ВПО «АлтГУ», 2015. – 5 с.
25. Короленко Ц.П. Семь путей к катастрофе: деструктивное поведение в современном мире / Ц.П. Короленко, Т.А. Донских. – Новосибирск: Наука, 1990. – 224 с.
26. Крюкова И.В. Фишинг как вид интернет-мошенничества / И.В. Крюкова, Э.Н. Алимамедов // Наукосфера. – 2021. – № 2-2. – С. 196-201.
27. Левин Л.М. Психофизиологические и психиатрические аспекты интернет-зависимости / Л.М. Левин // Научное мнение. – 2020. – № 5. – С. 68-78. [Электронный ресурс] – URL: <https://www.elibrary.ru/item.asp?id=43100895>
28. Леонов А.В., Назаренко А.Я. Проблемы предупреждения преступлений с использованием сети Интернет // Закон и право. 2018. №8. URL: <https://cyberleninka.ru/article/n/problemy-preduprezhdeniya-prestupleniy-s-ispolzovaniem-seti-internet> (дата обращения: 27.02.2022).
29. Лопатина Я.В. Социально-педагогические технологии работы с наркозависимыми подростками / Я.В. Лопатина // Ученые записки Российского государственного социального университета. – 2012. – №7. – С. 58-62.
30. Луков В.А. Травля в школах по-старому и по-новому (кибербуллинг) / В.А. Луков // Образовательные технологии (г. Москва). – 2019. – № 3. – С. 47-53.
31. Мамедов А.К. Подросток в системе «Человек-Машина»: интернет-аддикция и девиантные формы поведения / А.К. Мамедов // Миссия конфессий. – 2021. – Т. 10. – № 7(56). – С. 727-741. [Электронный ресурс] – URL: <https://www.elibrary.ru/item.asp?id=47631562>
32. Мертон Р.К. Социальная структура и аномия // СОЦИС, 1992. № 2. – С. 104–128.

33. Мигунова А.В. Возможности социальной работы в решении школьных проблем // Вестник Нижегородского университета им. Н.И. Лобачевского: Серия социальные науки. – 2013. – №4 (32). – С. 62-67.
34. Могунова М.М. Технология осуществления и правовая регламентация незаконного овладения персональными банковскими данными (фишинг) / М.М. Могунова // Вестник Саратовской государственной юридической академии. – 2020. – № 4(135). – С. 135-141. – DOI 10.24411/2227-7315-2020-10110.
35. Нафталиева В.О. Влияние современных СМИ на молодежь / В.О. Нафталиева // Философские проблемы информационных технологий и пространства. – 2011. – № 2. – С. 1-14.
36. Окунева Л.И. Факторы, обуславливающие формирование кибераддикции у подростков / Л.И. Окунева // Педагогическое образование в России. – 2016. – № 2. – С. 157-162.
37. Плешаков В.А. Теория киберсоциализации человека / В.А. Плешаков. – М.: Изд-во МПГУ; «НомоCyberus», 2011. – 361 с.
38. Расторгуев А.Ю. К вопросу о киберрискованном онлайн-поведении несовершеннолетних подростков / А.Ю. Расторгуев // Проблемы современного педагогического образования. – 2021. – № 71-3. – С. 362-366.
39. Семенов М.Ю. Мошенничество в сети Интернет: отношение молодежи / М.Ю. Семенов, П.В. Качанова // Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. – 2021. – Т. 7. – № 3(27). – С. 71-85. – DOI 10.21684/2411-7897-2021-7-3-71-85.
40. Солдатов Г.У., Ярмина А.Н. Кибербуллинг: особенности, ролевая структура, детско-родительские отношения и стратегии совладания // Национальный психологический журнал. 2019. №3 (35) [Электронный ресурс] – URL: <https://cyberleninka.ru/article/n/kiberbulling-osobennosti-rolvaya-struktura-detsko-roditelskie-otnosheniya-i-strategii-sovladaniya> (дата обращения: 26.02.2022).
41. Сорокина К.О. Современное состояние проблемы индивидуально-психологических особенностей личности подросткового возраста с киберзависимостью / К.О. Сорокина // E-Scio. – 2020. – № 5(44). – С. 727-732. [Электронный ресурс] – URL: <https://www.elibrary.ru/item.asp?id=42988994>
42. Тагильцева Ю.Р. Интернет-механизмы вовлечения в экстремистские сообщества / Ю.Р. Тагильцева, И.В. Воробьева, О.В. Кружкова [и др.] // Российский психологический журнал. – 2019. – Т. 16. – № 1. – С. 189-218.
43. Теохаров А.К. Киберпопрошайничество // Виктимология. 2020. №1 (23). URL: <https://cyberleninka.ru/article/n/kiberpoproshaynichestvo> (дата обращения: 27.02.2022).
44. Чернышева А.В. Фишинг как угроза современному информационному обществу / А.В. Чернышева, С.И. Самойлов // Научный потенциал. – 2021. – № 3(34). – С. 131-136.
45. Шейнов В.П. Опросник «Оценка степени незащищенности индивидов от кибербуллинга»: разработка и предварительная валидизация / В.П. Шейнов // Вестник Российского университета дружбы народов. Серия:

Психология и педагогика. – 2020. – Т. 17. – № 3. – С. 521-541.

46. Штайгер А.А. Социальная инженерия на примере фишинга / А.А. Штайгер // Вестник современных исследований. – 2018. – № 6.3(21). – С. 612-614.

47. Юрьева Л.Н., Бальбот Т.Ю. Компьютерная зависимость: формирование, диагностика, коррекция и профилактика: Монография. – Днепропетровск: Пирог, 2006. – 196 с.

48. Якушева В.С. Причины и последствия возникновения интернет-зависимости в старшем подростковом возрасте / В.С. Якушева // Информация и образование: границы коммуникаций. – 2014. – №6 (14). – С. 224-227.

Интернет-ресурсы (рекомендованные сайты)

<http://www.fom.ru> – Фонд «Общественное мнение»

<http://elibrary.ru> – Бесплатная электронная научная библиотека eLIBRARY

<http://www.gks.ru/> – Федеральная служба государственной статистики

<http://www.rosmintrud.ru/> – Министерство труда и социальной защиты РФ

<http://www.minsocium.ru/> – Министерство социальной политики нижегородской области

9. Материально-техническое обеспечение курса

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой, оснащенные оборудованием и техническими средствами обучения: переносными проектором и экраном для демонстрации презентаций.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечены доступом в электронную информационно-образовательную среду.

Заключение

Самореализация личности с зависимостью от Интернета замедляется, навыки реального общения не развиваются, а вместе с ними тают шансы на удачную адаптацию в учебном заведении, успешное трудоустройство и поиск партнера для создания семьи. Чрезмерное увлечение гаджетами может приводить к серьезным нарушениям здоровья, поэтому крайне важно, чтобы исследования на предмет выявления склонности к интернет-зависимости проводились во всех городах России, во всех учебных заведениях регулярно, только так можно организовать качественную и своевременную профилактику рисков для здоровья российской молодежи.

Ассоциация выпускников ННГУ, с помощью ученых факультета социальных наук, провела исследование уровня сетевой грамотности нижегородской молодежи в 2021 г. и 2022 г. Интернет-вовлеченность городской молодежи Нижнего Новгорода оказалась высокой. Молодое поколение не представляет свой день без компьютера и электронных гаджетов: 43% совокупно проводят в сети от 6 до 10 часов, 32% – 3-5 часов, 14% – 1-2 часа, 9% – более 12 часов и 2% – не определились с затраченным на это временем.

Сетевая грамотность и навыки в сфере кибербезопасности оценивались по четырем группам: устойчивость к киберзависимости, кибербуллингу, фишингу, кибермошенничеству. В целом, молодые люди продемонстрировали средний уровень устойчивости к киберзависимости. Социальные сети остаются для молодежи пространством конфликта: 78% получали в сети Интернет неприятные сообщения или комментарии, 91% – приходилось добавлять кого-то в черный список; 71% – с кем-то спорили в социальных сетях или на форумах. Серьезной угрозой для молодежи остается фишинг данных и другие формы интернет-мошенничества. 61% опрошенных открывали письма от неизвестных пользователей, 56% получали письма с просьбой сообщить свои персональные данные.

Подводя итог, отметим, что сегодня проблема киберзависимости остается для нижегородской молодежи достаточно актуальной. Однако на первое место постепенно выдвигаются киберугрозы другого характера: кибермошенничество, фишинг данных, навязывания товаров и услуг в сети. Однако перед проведением обучения кибербезопасности необходимо регулярно обновлять данные мониторинга.

Учебно-методическое пособие подготовлено в рамках проекта «Сетевая грамотность нижегородской молодежи: механизмы мониторинга и технологии развития» по реализации подпрограммы «Поддержка социально ориентированных некоммерческих организаций в Нижегородской области» государственной программы «Социальная поддержка граждан Нижегородской области», утвержденной постановлением Правительства Нижегородской области от 30 апреля 2014 г. № 298, при софинансировании Фонда президентских грантов.

Приложение 1. Технологическая карта сетевых угроз

<i>Название</i>	<i>Характеристика</i>	<i>Виды</i>	<i>Способы противодействия</i>	<i>Степень угрозы</i>
Киберзависимость	<p>Психосоциальная проблема, проявляющаяся в навязчивом желании использовать Интернет без контроля проведенного в нем времени, что приводит к разрыву или потере социальных связей с окружением и замене реальных отношений и интересов виртуальными.</p> <p>Признаки киберзависимости: отказ от реального общения ради досуга в сети, раздражение в случае долгого отсутствия доступа к сети Интернет, конфликты по поводу использования компьютера и Интернета, пренебрежение правилами личной гигиены и распорядком питания, сна, потребность в бесцельном длительном потреблении информации в сети Интернет (некритичное длительное бесцельное чтение информации в Интернете).</p>	<p>Интернет-гемблинг, Интернет-гейминг, Интернет-хакерство, Интернет-шопоголизм, Интернет-серфинг, киберкоммуникативность.</p>	<p>Вовлечение в социально полезную деятельность, развитие навыков тайм-менеджмента, помощь психолога в разрешении межличностных проблем</p>	средний
Кибербуллинг	<p>Агрессивное преследование индивида с использованием</p>	<p>Кибермоббинг, Троллинг</p>	<p>В случае обнаружения первых признаков</p>	высокий

	цифровых технологий в течение продолжительного периода времени.	линг, Диссинг, Фрейпинг, Кэтфинг	онлайн-травли нужно немедленно обратиться к администратору сообщества или веб-сайта с просьбой удалить нежелательный контент; не отвечать на подозрительные сообщения, повысить сложность паролей своего профиля, не передавать/не публиковать личные данные, блокировать агрессора.	
Фишинг	Вид интернет-мошенничества с целью получения логина и пароля для доступа к персональным данным, в том числе финансовым. В большинстве случаев фишинг представлен в виде массовых рассылок писем и уведомлений от известных брендов, почтовых систем, банков, социальных сетей. Мошенники размещают в письме логотип организации, сообщение и прямую ссылку на сайт, который не имеет внешних отличий от	Рассылка писем с вирусами, фарминг (секретное перенаправление пользователя на зараженный сайт без его ведома), смишинг (атаки с помощью смс), вишинг (атаки с помощью телефонных звонков) и др.	Смена паролей, проверка источников информации, периодическая проверка аккаунтов, изучение информации о вредоносных программах.	средний

	<p>настоящего, на поддельном сайте требуется ввести конфиденциальные данные в соответствующие формы. Таким образом мошенники получают доступ к банковским счетам и учетным записям.</p>			
<p>Кибермошенничество</p>	<p>Хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием с использованием цифровых технологий.</p>	<p>Хищение личных данных, мошенничество в сфере интернет-банкинга, Интернет-прошайничество, продажа поддельных товаров в чрез поддельные интернет магазины</p>	<p>Защита аккаунтов осуществляется созданием сложных паролей, отказ от перехода на неизвестные сайты платежных систем, интернет-магазинов по ссылкам из непроверенных ранее источников. если к Вам обратились по телефону, в интернете, через социальные сети или другими способами, и под различными предлогами пытаются узнать данные о вашей банковской карте, код, пришедший на ваш мобильный телефон, или другую персональную информацию, прекратите звонок</p>	<p>высокий</p>

Роман Викторович Голубин
Инна Александровна Исакова
Александр Павлович Коротышев
Павел Павлович Рыхтик

**КИБЕРБЕЗОПАСНОСТЬ ПОДРОСТКОВ В СЕТИ ИНТЕРНЕТ.
ПРОТИВОДЕЙСТВИЕ КИБЕРУГРОЗАМ**

Учебно-методическое пособие

Федеральное государственное автономное образовательное учреждение
высшего образования «Национальный исследовательский
Нижегородский государственный университет им. Н.И. Лобачевского»
603950, Нижний Новгород, пр. Гагарина, 23.