



**БЕЗОПАСНАЯ
МОЛОДЁЖНАЯ СРЕДА**
программа от росмолодёжи



**БАЛТИЙСКИЙ
ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
ИМЕНИ ИММАНУИЛА КАНТА**

В. В. Балановский

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
И МАТЕРИАЛЫ ПО ИНФОРМАЦИОННОЙ ГИГИЕНЕ
В МОЛОДЕЖНОЙ СРЕДЕ**

Учебное электронное издание

**Издательство
Балтийского федерального университета им. Иммануила Канта
2023**

© Федеральное агентство по делам молодежи, 2023

Рецензенты

Е. Р. Россинская, доктор юридических наук, профессор, научный руководитель Института судебных экспертиз, заведующая кафедрой судебных экспертиз Московского государственного юридического университета им. О. Е. Кутафина (МГЮА), заслуженный деятель науки РФ;

В. А. Мещеряков, доктор юридических наук, кандидат технических наук, профессор, профессор кафедры криминалистики Воронежского государственного университета

Об авторе

Балановский Валентин Валентинович, кандидат философских наук, начальник отдела аналитики, мониторинга и по связям с общественностью комитета по связям с общественностью и средствами массовой информации администрации городского округа «Город Калининград», старший научный сотрудник ОНК «Институт образования и гуманитарных наук» БФУ им. И. Канта

Балановский, В. В.

Методические рекомендации и материалы по информационной гигиене в молодежной среде [Электронный ресурс] : учебное электронное издание / В. В. Балановский. — Калининград : Издательство БФУ им. И. Канта, 2023. — 40 с.

Разработаны в целях оказания содействия в организации и проведении профилактических мероприятий, направленных на формирование и развитие у граждан в возрасте от 14 до 35 лет навыков информационной гигиены как в рамках образовательного процесса, так и за его пределами.

Ориентированы на лиц, работающих с молодежью в организациях сферы образования, спорта, культуры, молодежной и социальной политики, а также могут представлять интерес для широкого круга лиц.

Методические рекомендации подготовлены в БФУ им. И. Канта по заказу Федерального агентства по делам молодежи

СОДЕРЖАНИЕ

| | |
|---|----|
| Резюме | 4 |
| Введение | 5 |
| Алгоритм профилактической работы в сфере информационной гигиены | 11 |
| Правовое обеспечение профилактической работы в сфере информационной гигиены | 20 |
| Виды и формы профилактических мероприятий | 22 |
| Обобщение положительного опыта формирования информационной гигиены в молодежной среде | 30 |
| Основные выводы | 37 |
| Заключение | 38 |
| Список рекомендуемой литературы | 39 |

РЕЗЮМЕ

Комплекс методических рекомендаций и информационных материалов разработан в целях оказания содействия в организации и проведении профилактических мероприятий, направленных на формирование и развитие у граждан в возрасте от 14 до 35 лет умений и навыков информационной гигиены как в рамках образовательного процесса, так и за его пределами. Рекомендации ориентированы на лиц, работающих с молодежью в организациях сферы образования, спорта, культуры, молодежной и социальной политики, а также могут представлять интерес для широкого круга лиц.

Методические рекомендации предваряются теоретической частью, в которой дается общее представление об информационной гигиене как совокупности компетенций, позволяющих обеспечить безопасность взаимодействия индивида с информационной средой и направленных на формирование умений и навыков осознанного и ответственного потребления и производства (распространения) информации. Также приводится характеристика современного состояния взаимодействия граждан с информационной средой в Российской Федерации с опорой на социологические данные.

В основной части методических рекомендаций помимо общего алгоритма профилактической работы в сфере информационной гигиены представлено описание правовой базы с указанием нормативно-правовых актов, наиболее часто используемых в профилактической работе специалистами в данной сфере; дается краткий обзор наиболее эффективных конкретных видов и форм профилактических мероприятий, реализуемых как в рамках учебного процесса, так и за его пределами; приводятся успешные примеры апробированных методов работы с молодежью по формированию навыков информационной гигиены.

Кроме того, методические рекомендации снабжены описанием положительного опыта регионов по формированию информационной гигиены в молодежной среде с указанием ссылок, по которым можно найти полезные материалы, готовые к использованию в профилактической работе.

ВВЕДЕНИЕ

Цивилизационные вызовы таковы, что в условиях возрастания роли массовой коммуникации, развития технологий информационного воздействия на индивидов, ведения когнитивных войн навыки соблюдения информационной гигиены должны стать базовой компетенцией каждого гражданина России. В особенности негативному влиянию информационной среды подвержены выросшие в цифровую эпоху молодые люди. Обусловлено это тем, что современная молодежь не испытывала трудностей с получением доступа к любой информации, из-за чего, как правило, не имеет опыта ее самостоятельного поиска, верификации, определения круга и качества ее источников, а также тем, что дети и подростки стали слишком рано переходить на аудиовизуальную информационную продукцию, что привело к сокращению объемов чтения и в целом к снижению способности понимать и анализировать текст¹. Кроме того, как отмечалось выше, на месте не стоят технологии информационного воздействия — от разработок в сфере подростковой психологии и психологии восприятия до развития нейросетей и систем искусственного интеллекта, позволяющих на качественном уровне осуществлять фальсификацию текстового и аудиовизуального контента.

Несмотря на сравнительно недавнее появление информационной гигиены, это явление имеет длительную историю изучения российскими учеными, в том числе философами права и психологами², и с каждым днем все прочнее закрепляет свои позиции в научном, педагогическом и общественно-политическом дискурсах. Последнее особенно большое значение приобрело в контексте проведения специальной военной операции на Украине (далее — СВО) по причине того, что противодействующие Российской Федерации силы активно используют методы информационного воздействия, в том числе направленные против российской молодежи.

Так, согласно данным председателя Национального антитеррористического комитета, директора ФСБ России А. В. Бортникова, с февраля 2022 года по апрель 2023 года в нашей стране было предотвращено 118 преступлений террористической направленности, исполнителями которых были молодые люди и

¹ Ломбина Т. Н., Мансуров В. А., Юрченко О. В. Проблемы чтения в новой цифровой реальности (на примере школьников). Часть 2 // Социологическая наука и социальная практика. 2020. Т. 8, № 1. С. 93—105. doi: 10.19181/snsp.2020.8.1.7097.

² Балановский В. В. Роль информационной гигиены в условиях санитарно-эпидемиологических ограничительных мер // Современные технологии и подходы в юридической науке и образовании. Калининград : Изд-во БФУ им. И. Канта, 2021. С. 362—363.

подростки, среди них несовершеннолетние¹. Во многом такое количество преступление стало результатом вербовочной работы украинских спецслужб и их помощников с использованием дистанционных средств коммуникации, прежде всего посредством сети Интернет.

Кроме того, с началом СВО, по данным банковских аналитиков, основная часть телефонных мошенничеств стала осуществляться с территории Украины, а одной из ключевых целей подобных преступлений является отъем у граждан России денежных средств и направление их на финансирование Вооруженных сил Украины². Причем, что примечательно, в большинстве случаев жертвами мошенничеств с использованием дистанционных средств коммуникации становятся не пенсионеры, случаи обмана которых наиболее активно освещаются в средствах массовой информации, а молодежь и трудоспособное население в возрасте от 14 до 44 лет, которые, согласно данным Центрального банка Российской Федерации (Банка России), в 2022 году становились жертвами злоумышленников в 55,3 % случаев³ (в основном это телефонные мошенничества, занимающие 60 % от общего объема правонарушений данного характера) (табл. 1). Причем в 2022 году 17 % из общего числа пострадавших пришлось на учащихся⁴.

Таблица 1

**Категории граждан, наиболее уязвимых
к действиям финансовых мошенников**

| Возраст, лет | Доля опрошенных, % |
|--------------|--------------------|
| 14—19 | 10,3 |
| 20—24 | 7,6 |
| 25—44 | 37,4 |
| 45—64 | 29 |
| 65 + | 15,7 |

Важно также подчеркнуть, что мы живем в эпоху комбинированных угроз, нивелирование которых требует усиленной и четко скоординированной меж-

¹ Председатель Национального антитеррористического комитета Бортников провел заседание НАК // Национальный антитеррористический комитет. URL: <http://nac.gov.ru/nak-prinimaet-resheniya/predsedatel-nacionalnogo-antiterroristicheskogo-komiteta.html> (дата обращения: 11.04.2023).

² Мошеннический кол-центр «Бердянск» // СберБанк. URL: <http://www.sberbank.ru/ru/person/kibrary/investigations/berdyansk> (дата обращения: 13.05.2023).

³ Обзор операций, совершенных без согласия клиентов финансовых организаций // Банк России. URL: http://www.cbr.ru/analytics/ib/operations_survey_2022/ (дата обращения: 13.05.2023).

⁴ Там же.

ведомственной работы. Яркий пример — информационные эпидемии, или инфодемии. Данный термин появился впервые в контексте стремительного распространения атипичной пневмонии. Однако особенно популярным он стал в контексте появления коронавирусной инфекции COVID-19. Информационная эпидемия — это лавинообразное распространение достоверной и недостоверной информации по определенной тематике, связанной с непосредственной угрозой здоровью и жизни человека. Масштабность информационных эпидемий обеспечивается сочетанием нескольких угрожающих факторов:

- наличием реальной угрозы здоровью и жизни человека, что вызывает страх у потребителей информации, тем самым выводит их из эмоционального равновесия и не позволяет объективно оценивать обстановку;

- легкостью распространения информации, в том числе недостоверной;

- проблемами, связанными с координацией действий организаций и лиц, ответственных за решение проблемы, вокруг которой консолидируется информационная эпидемия, и за наполнение информационного поля;

- отсутствием у индивидов элементарных навыков информационной гигиены.

В результате информационная эпидемия приводит к дезориентации потребителей информации, поскольку они не знают, какому источнику доверять, как самостоятельно оценить достоверность источника или компетенцию инфлюенсера, а также какими рекомендациями и требованиями руководствоваться.

В результате объективной оценки высокого уровня угроз, связанных с воздействием информационной среды на подрастающее поколение, в России стали появляться общественные инициативы, ставящие целью просвещение в области информационной безопасности и информационной гигиены среди детей и молодежи, а также начало активно развиваться законодательство в данной сфере. Так, в 2011 году появилась Ассоциация участников рынка интернет-индустрии «Лига безопасного Интернета», основная цель которой — создание безопасного пространства Интернета на территории Российской Федерации¹. Также к этой работе подключились крупнейшие отечественные компании финансового IT-сектора, запускающие просветительские проекты в сфере кибербезопасности, в том числе ориентированные непосредственно на детей и подростков. Кроме того, в Государственной думе ФС РФ с 2019 года стали озвучиваться предложения по введению в школах обязательных уроков по информационной безопасности².

¹ Лига безопасного Интернета. URL: <https://ligainternet.ru/> (дата обращения: 13.05.2023).

² В ГД предложили ввести в школах изучение информационной безопасности // Государственная дума Федерального собрания Российской Федерации. URL: <http://duma.gov.ru/news/45603/> (дата обращения: 13.05.2023) ; В Госдуме предложили внедрить в школы «цифровую гигиену» // Московский комсомолец. URL: <https://www.mk.ru/social/2022/12/29/v-gosdume-predlozhili-vnedrit-v-shkoly-cifrovuyu-gigienу.html> (дата обращения: 12.04.2023).

В контексте совершенствования работы по обеспечению безопасности взаимодействия молодежи с информационной средой ключевым событием в сфере законодательства стало издание распоряжения Правительства Российской Федерации от 28 апреля 2023 года № 1105-р, которым утверждена Концепция информационной безопасности детей в Российской Федерации. В частности, некоторыми принципами, из которых исходит Концепция, являются необходимость формирования у детей умения ориентироваться в современной информационной среде; воспитание у них навыков самостоятельного и критического мышления; обучение детей вопросам информационной безопасности. Таким образом, привитие информационной гигиены в молодежной среде в полной мере отвечает указанным принципам, а также способствует решению озвученных в Концепции приоритетных задач.

Данные методические рекомендации разработаны с **целью** формирования представления о базовых правилах информационной гигиены и их использования для обеспечения безопасности взаимодействия молодежи с информационной средой, а также для ознакомления с конкретными практическими методами развития навыков информационной гигиены у молодых людей.

Методические рекомендации ориентированы на широкий круг лиц, которые работают с молодежью в организациях сферы образования, спорта, культуры, молодежной и социальной политики, а также на родителей, заинтересованных в привитии своим детям навыков информационной гигиены.

Результатом внедрения данных методических рекомендаций должно стать:

— ознакомление с базовыми правилами информационной гигиены и их практическим использованием в целях обеспечения безопасности взаимодействия с информационной средой;

— формирование компетенций в сфере развития навыков информационной гигиены у молодежи;

— повышение эффективности профилактической работы среди молодежи в сфере информационной гигиены, в том числе за счет ознакомления с общими алгоритмами действий и реализованными конкретными практиками из различных субъектов Российской Федерации.

Прежде чем перейти к описанию алгоритма профилактической работы, следует дать определение понятию информационной гигиены во избежание двоякого толкования этого термина, а также разграничить его со схожими по смыслу понятиями информационной безопасности, кибербезопасности, медиаэкологии или информационной экологии.

Безусловно, за основу можно взять определение, сформулированное ФБУЗ «Центр гигиенического образования населения» Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека. Оно гласит, что «информационная гигиена — раздел медицинской науки, изучающий закономерности влияния информации на психическое, физическое и социальное благополучие человека, его работоспособность, продолжительность жизни, общественное здоровье социума, разрабатывающий нормативы и мероприятия

по оздоровлению окружающей информационной среды и оптимизации интеллектуальной деятельности»¹. Также на сайте Центра содержатся практические правила информационной гигиены. Их всего три:

- «1) телевизор включать по мере необходимости;
- 2) в сеть только с целью;
- 3) информационно-разгрузочные дни»².

Вместе с тем, несмотря на удобство приведенного определения и простоту предлагаемых правил, они не в полной мере отвечает современным реалиям. В первую очередь в том отношении, что они не учитывают специфику поведения индивидов в информационной среде. С развитием интернет-технологий индивиды стали не только пассивными потребителями информации, но и активными ее распространителями и производителями (рис. 1). Последние два момента за последние годы стали все чаще находить отражение в новеллах российского законодательства и правоприменительной практике. Поэтому, формулируя правила информационной гигиены и разрабатывая методы ее формирования в молодежной среде, следует отразить и другую — субъект-активную — сторону вопроса.

Исходя из поставленной задачи, целесообразно дать следующее определение: **информационная гигиена — это совокупность компетенций, позволяющих обеспечить безопасность взаимодействия индивида с информационной средой и направленных на формирование умений и навыков осознанного и ответственного потребления и производства (распространения) информации.**



Рис. 1. Векторы применения информационной гигиены

В соответствии с данным определением правила информационной гигиены будут касаться трех базовых умений и навыков (рис. 2):

- 1) верификации информации;
- 2) защиты персональных данных и данных доступа;
- 3) ответственного поведения в публичном пространстве.

¹ Информационная гигиена // ФБУЗ «Центр гигиенического образования населения» Роспотребнадзора. URL: <https://cgon.rospotrebnadzor.ru/naseleniyu/zdorovyuy-obraz-zhizni/informatsionnaya-gigiena/> (дата обращения: 12.04.2023).

² Там же.

В соответствии с указанными умениями будут варьироваться угрозы, против которых должны быть направлены навыки информационной гигиены.



Рис. 2. Базовые умения и навыки информационной гигиены

АЛГОРИТМ ПРОФИЛАКТИЧЕСКОЙ РАБОТЫ В СФЕРЕ ИНФОРМАЦИОННОЙ ГИГИЕНЫ

Профилактическая работа, направленная на формирование умений и навыков информационной гигиены, должна начинаться с четкого понимания **субъекта, объекта, целей, средств и результатов** данной деятельности (рис. 3). Кроме того, следует представлять спектр угроз, которым призвана противостоять информационная гигиена и которые будут подробнее охарактеризованы ниже. Также важно помнить, что только жесткая привязка к практикам современной повседневности, касающимся каждого индивида, взаимодействующего с информационной средой, только указание конкретных примеров из жизни, связанных с нарушением законных прав и свобод гражданина, могут обеспечить подлинный интерес целевой аудитории проводимой работы.



Рис. 3. Структура профилактической работы

При этом при выборе конкретных профилактических средств необходимо учитывать то, что современная молодежь реже читает, информацию предпочитает получать посредством сети Интернет, преимущественно через социальные сети или видеоплатформы. Так, согласно проведенному после блокировки ряда популярных иностранных платформ в 2022 году опросу¹, чаще всего молодые люди в возрасте от 14 до 22 лет проводили время в соцсети *ВКонтакте* — 69,44 % опрошенных, следующим по популярности стали *YouTube* — 57,41 %, *Instagram*² — 54,63 %, *TikTok* — 47,22 %. При этом подавляющее большинство опрошенной молодежи пользовалось мессенджером Telegram (93 %) (табл. 2).

¹ Какие соцсети предпочитают подростки в России и Беларуси // RG.RU. Союз Беларусь / Россия. 26.10.2022. URL: <https://rg.ru/2022/10/26/kakie-socseti-predpochitaiut-podrostki-v-rossii-i-belarusi.html> (дата обращения: 12.04.2023).

² Принадлежит *Meta* — организации, деятельность которой признана экстремистской и запрещена на территории РФ.

Таблица 2

**Самые популярные площадки и сервисы в сети Интернет среди молодежи,
по данным агентства «Интериум» за 2022 год**

| Интернет-площадка | Доля опрошенных, % |
|-------------------|--------------------|
| Telegram | 93 |
| ВКонтакте | 69,44 |
| YouTube | 57,41 |
| Instagram | 54,63 |
| TikTok | 47,22 |

Все это в очередной раз подчеркивает особенности восприятия современных молодых людей, которые предпочитают видео и изображения тексту, короткие тексты лонгридам. Соответственно, в профилактических целях большим дидактическим потенциалом обладают инфографика и ролики, особенно если они сделаны с юмором, поскольку, согласно исследованию Всероссийского центра изучения общественного мнения¹, именно юмористический контент больше всего привлекает в Интернете молодых людей в возрастных группах от 18 до 24 лет (49 % опрошенных) и с 25 до 34 лет (43 %) (табл. 3).

Таблица 3

Популярные категории контента среди молодежи, %

| Категория | Возраст | |
|-----------------------------|------------|------------|
| | 18—24 года | 25—34 года |
| Юмор | 49 | 43 |
| Здоровье | 35 | 38 |
| Новости о событиях в стране | 32 | 40 |
| Еда, рецепты | 34 | 35 |
| Семья, дети, дом | 28 | 39 |
| Путешествия | 39 | 36 |
| Спорт | 44 | 33 |
| Наука, техника | 36 | 31 |

¹ Социальные сети: кто туда ходит и зачем? // Сайт ВЦИОМ. Запись от 02.06.2017. URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/soczialnye-seti-kto-tuda-khodit-i-zachem> (дата обращения: 13.05.2023).

| Категория | Возраст | |
|---|------------|------------|
| | 18—24 года | 25—34 года |
| Образование, саморазвитие | 35 | 26 |
| Автомобили, мотоциклы | 26 | 30 |
| Политика | 14 | 22 |
| Животные | 26 | 23 |
| Искусство и культура | 21 | 18 |
| Покупки | 25 | 24 |
| Мода, стиль, красота | 32 | 25 |
| Экономика, финансы, бизнес | 17 | 22 |
| Психология, мотивы | 25 | 18 |
| Территориальные группы (мой город, район и пр.) | 13 | 15 |
| Профессиональные группы | 14 | 15 |
| Учебные группы (вуз, школа и пр.) | 21 | 15 |
| Другое | 1 | 0 |
| Ни в одной из групп | 0 | 1 |
| Затрудняюсь ответить | 0 | 0 |

1. **Субъектом** профилактической деятельности, направленной на формирование умений и навыков информационной гигиены, как правило, выступает лицо, которое уполномочено работать с молодежью в организациях сферы образования, спорта, культуры, молодежной и социальной политики, или родители. Учитывая активное развитие в Российской Федерации форм просветительской работы, в том числе под эгидой Российского общества «Знание» и других некоммерческих организаций, субъектом профилактики могут также выступать различные лекторы или представители некоммерческих организаций, распространяющие просветительский контент в сфере информационной гигиены.

В случае если субъектом профилактики являются сотрудники государственных и муниципальных учреждений образования, культуры, молодежной политики, спорта и др., целесообразно закрепить за данными сотрудниками соответствующие должностные обязанности. Также следует разработать годовой план профилактических мероприятий.

Объектом профилактической работы, направленной на формирование умений и навыков информационной гигиены, выступают молодые люди в возрасте от 14 до 35 лет, в первую очередь учащиеся учебных заведений общего, среднего специального и высшего образования, воспитанники молодежных клубов, члены молодежных общественных организаций.

Целью профилактической работы является формирование умений и навыков информационной гигиены сообразно угрозам, на защиту от которых они

направлены. В первую очередь это умения и навыки верификации информации, защиты персональных данных и данных доступа, ответственного поведения в публичном пространстве.

Средствами профилактической работы выступают конкретные виды просветительских, образовательных, воспитательных мероприятий (уроки, презентации, деловые игры, квесты, квизы, хакатоны), а также дополнительные программные и аудиовизуальные средства, используемые в профилактической работе (инфографика, видеоролики, мобильные приложения, специализированное программное обеспечение, тематические сайты, каналы и чат-боты).

В качестве **целевых показателей** могут быть установлены следующие конкретные измеримые результаты:

— количество проведенных профилактических мероприятий в сфере информационной гигиены;

— количество участников из числа молодежи, принявших участие в данных профилактических мероприятиях в сфере информационной гигиены;

— количество лиц, уполномоченных работать с молодежью в организациях сферы образования, спорта, культуры, молодежной и социальной политики, и родителей, прошедших курсы по изучению правил и формированию умений и навыков информационной гигиены, включая курсы повышения квалификации;

— количество средств, затраченных на проведение профилактических мероприятий в сфере информационной гигиены.

Выбор средств обеспечения информационной гигиены должен осуществляться сообразно базовой группе умений и навыков в зависимости от характера конкретных угроз (рис. 4).



Рис. 4. Общий алгоритм выбора средств информационной гигиены

2. Умения и навыки, связанные с **верификацией информации**, позволяют нивелировать такие угрозы, как производство и распространение ложной или непреднамеренно либо преднамеренно искаженной текстовой или аудиовизуальной информации. Примерами подобных манипуляций являются фейки (фейк-ньюс, технология deepfake), дезинформация, розыгрыши (пранки).

При выборе средств формирования умений и навыков верификации информации следует ориентироваться на методы, развивающие способность к критическому восприятию и анализу информации, а также дающие базовые навыки работы со специальными техническими средствами (табл. 4). В част-

ности, для разоблачения фейк-ньюс могут использоваться обычные популярные поисковые системы для поиска источника искаженной или ложной информации, первоисточников фото-, аудио- и видеоконтента, сопоставления информации об одних и тех же событиях из разных источников информации. Кроме того, сегодня существуют специальные интернет-сообщества, занимающиеся разоблачением фейков, например телеграм-канал «Война с фейками» или сайт «Лапша медиа», где есть даже форма анонимной обратной связи, через которую можно подать предположительно фейковую информацию для проверки специалистами. Подобные интернет-ресурсы стали особенно популярными и востребованными с началом СВО, спровоцировавшей вал дезинформации со стороны противников Российской Федерации. Кроме того, существует специальное программное обеспечение, работающее и онлайн, которое позволяет выявлять источники происхождения текстовой и аудиовизуальной информации, анализировать текст на плагиат, фото на факт наличия ретуши, звук и видео на наличие монтажа или подделок, в том числе с использованием технологии deepfake.

Таблица 4

Верификация информации: угрозы и средства противостояния

| СФЕРА | УГРОЗЫ | СРЕДСТВА |
|-----------------------------------|--|---|
| ВЕРИФИКАЦИЯ ИНФОРМАЦИИ | Дезинформация Фейки (фейк-ньюс, технология deepfake) Информационные эпидемии Розыгрыши (пранки) | Способность к критическому восприятию и анализу информации Тематические интернет-ресурсы Специализированное программное обеспечение по анализу текстового и аудиовизуального контента и др. |

3. Умения и навыки, связанные с **защитой персональных данных и данных доступа**, позволяют нивелировать такие угрозы, как мошенничество, кража персональных данных и данных доступа, кража денежных средств, сбор компрометирующей информации, вербовка в деструктивные сообщества, интернет-шантаж, шпионаж посредством сбора данных из открытых источников (технологии OSINT — Open Source Intelligence) (табл. 5).

Защита данных: угрозы и средства противостояния

| СФЕРА | УГРОЗЫ | СРЕДСТВА |
|--|--|--|
| ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ И ДАННЫХ ДОСТУПА | Мошенничество Кража персональных данных и данных доступа Сбор компрометирующей информации Вербовка в деструктивные сообщества Шантаж и кибербуллинг Шпионаж (технологии OSINT — Open Source Intelligence) | Ответственное отношение к собственной персональной информации Использование специализированного защитного программного обеспечения Надежные пароли Двухфакторная аутентификация Настройка параметров приватности Использование надежного программного обеспечения и др. |

При выборе конкретных средств для формирования умений и навыков защиты персональных данных и данных доступа следует ориентироваться на методы, развивающие ответственное отношение молодежи к персональной информации, которую они выкладывают в открытый доступ или доступ к которой самостоятельно предоставляют третьим лицам или программному обеспечению, включая мобильные приложения. Акцент важно делать на том, что часто занимаемая индивидами пассивная позиция, согласно которой все, кому надо, и так все про нас знают и если какая-то IT-корпорация хочет собрать информацию о человеке, она это сделает, сегодня является заведомо проигрышной. В последние годы законодательство, в том числе международное, в сфере защиты прав на приватность стремительно развивалось. Поэтому крупнейшие IT-корпорации, включая разработчиков популярных поисковых и почтовых сервисов, социальных сетей и мессенджеров, вынуждены были предоставить возможность пользователям самостоятельно настраивать параметры приватности в сети, включая даже запрет на сбор обезличенных данных об онлайн-поведении индивидов.

Кроме того, важно дать понять, что именно сами пользователи сети Интернет предоставляют всю необходимую информацию экономического, юридического, социального, психологического характера о себе, которую собирают и анализируют мошенники и вербовщики с целью использования в противоправной деятельности, в том числе с использованием набирающих сегодня популярность методов OSINT.

Отдельного внимания заслуживает тема интернет-шантажа. Зачастую жертвами становятся лица, пытающиеся с помощью социальных сетей завести знакомство с целью налаживания личной жизни. В данном случае злоумышленники преимущественно используют поддельные аккаунты в соцсетях для получения интимных фото-, видеоизображений, с помощью которых затем шантажируют потерпевшего.

Равным образом компрометирующая или важная финансовая информация может попасть к преступникам в результате взлома аккаунта, а также из-за использования ненадежных сервисов, позволяющих обходить блокировку интернет-ресурсов (технологии VPN — virtual private network). Чаще всего это становится возможным из-за небрежного отношения к выбору пароля для учетной записи или игнорирования необходимости применения двухфакторной аутентификации.

4. Умения и навыки, связанные с **ответственным поведением в публичном пространстве**, в первую очередь интернет-пространстве, позволяют нивелировать такие угрозы, как непреднамеренное и преднамеренное изготовление и размещение противоправного контента, оскорбление различных социальных групп и категорий индивидов, разжигание конфликтов, а также наступление юридической ответственности за указанные действия.

При выборе конкретных средств для формирования умений и навыков, связанных с ответственным поведением в публичном пространстве, в первую очередь интернет-пространстве, акцент следует делать, во-первых, на том, что молодые люди являются не только активными потребителями, но также и распространителями и производителями информации, что накладывает на них определенную персональную ответственность, а во-вторых, на то, что законодательство в данной сфере весьма развито, а правоприменительная практика довольно интенсивна. Кроме того, важно довести до сознания молодых людей, что уровень анонимности в Интернете сегодня гораздо ниже, чем это было 10 лет назад, и сейчас гораздо проще определить распространителя противоправного контента, чем раньше. Поэтому ответственное отношение к производству и распространению информации даже на личных страницах в социальных сетях должно стать нормой поведения. Формироваться оно должно в первую очередь посредством правового просвещения (табл. 6).

**Ответственное поведение в публичном пространстве:
угрозы и средства противостояния**

| СФЕРА | УГРОЗЫ | СРЕДСТВА |
|---|---|--|
| <p align="center">ОТВЕТСТВЕННОЕ ПОВЕДЕНИЕ В ПУБЛИЧНОМ ПРОСТРАНСТВЕ</p> | <p align="center">Непреднамеренное и преднамеренное изготовление и размещение противоправного контента</p> <p align="center">Оскорбление различных социальных групп и категорий индивидов</p> <p align="center">Разжигание конфликтов</p> <p align="center">Наступление юридической ответственности за неправомерные действия</p> | <p align="center">Осознание персональной ответственности за поведение в сети Интернет</p> <p align="center">Правовое просвещение</p> <p align="center">Анализ правоприменительной практики</p> <p align="center">Контроль эмоций и др.</p> |

5. Следует помнить, что довольно сложно предсказать, какие в ближайшем будущем возникнут новые угрозы в сфере взаимодействия индивида и информационной среды. Так, каждый день появляются новые виды телефонных мошенничеств, сочетающих в себе использование специализированного программного обеспечения, современных технических средств и последних разработок в области психологии. Буквально сейчас формируются новые комплексные угрозы, связанные с возникновением интерактивных генеративных медиа — нового типа платформ по производству и распространению контента, созданных на основе нейросетей и позволяющих с помощью психологических и технических алгоритмов с использованием массива информации, собираемой о поведении индивидов в сети Интернет (big data), максимально незаметно для пользователя интегрировать отвечающую его запросам информацию, в том числе рекламного характера, которая будет восприниматься с минимальным сопротивлением со стороны пользователей¹. Это новый уровень развития технологий манипуляции сознанием, которые за счет больших вычислительных мощностей и быстро эволюционирующих систем искусственного интеллекта позволяют создавать предельно индивидуализированный информационный продукт.

¹ Why generative AI is more dangerous than you think // VentureBeat. URL: <https://venturebeat.com/ai/why-generative-ai-is-more-dangerous-than-you-think/?fbclid=IwAR1C-5Qebn8AHFVNceLCpeHrcP74hig3vUWTRx32GuKjZ7wZuCNJDSOkGkfg> (дата обращения: 15.05.2023).

С учетом сказанного следует помнить, что субъект профилактической деятельности в сфере информационной гигиены должен постоянно следить за появлением новых приемов информационного воздействия, повышать свою квалификацию и оперативно делиться своими знаниями с целевой аудиторией.

В заключение раздела дадим общую схему алгоритма профилактической деятельности (рис. 5). Итак, профилактическая деятельность в сфере информационной гигиены будет включать следующие шаги:

- 1) определение цели и конкретных задач профилактической деятельности;
- 2) определение целевой аудитории;
- 3) определение целевых показателей профилактической работы;
- 4) выбор форм и средств профилактической работы, релевантных для решения поставленных задач с учетом специфики целевой аудитории и угроз, против которых направлены принимаемые меры;
- 5) реализация конкретных профилактических мероприятий;
- 6) фиксация результатов профилактической деятельности, в том числе посредством получения обратной связи от целевой аудитории;
- 7) анализ достижимости целей и решаемости задач профилактической деятельности, а также эффективности выбранных форм и средств в контексте содержательного наполнения и достижения целевых показателей;
- 8) корректировка предыдущих шагов, исходя из результата произведенного анализа.



Рис. 5. Общий алгоритм профилактической деятельности

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ПРОФИЛАКТИЧЕСКОЙ РАБОТЫ В СФЕРЕ ИНФОРМАЦИОННОЙ ГИГИЕНЫ

Правовую основу профилактической работы в сфере информационной гигиены составляют различные нормативно-правовые акты и иные документы (инструкции, рекомендации, должностные инструкции, локальные приказы и т. д.), которые регулируют отношения в сфере взаимодействия индивидов и информационной среды, а также образовательную, просветительскую и воспитательную деятельность. Это тот минимум, который позволяет обеспечить максимальную эффективность и наименьший уровень риска при проведении профилактической работы, что крайне важно, когда речь идет о молодежи.

Несмотря на то что фактически таких нормативно-правовых актов и документов может быть крайне много, в зависимости от характера субъектов профилактической работы и особенностей целевой аудитории, как правило, чаще всего на практике в сфере формирования информационной гигиены используются следующие нормативно-правовые акты:

1. Конституция Российской Федерации.
2. Семейный кодекс Российской Федерации.
3. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию».
4. Федеральный закон «Об основных гарантиях прав ребенка в Российской Федерации».
5. Федеральный закон «Об информации, информационных технологиях и о защите информации».
6. Закон Российской Федерации от 27.12.1991 № 2124-1 «О средствах массовой информации».
7. Федеральный закон от 13.03.2006 № 38-ФЗ «О рекламе».
8. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».
9. Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму».
10. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи».
11. Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности».
12. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
13. Федеральный закон от 30.03.1999 № 52-ФЗ «О санитарно-эпидемиологическом благополучии населения».
14. Указ Президента Российской Федерации от 09.11.2022 № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей».
15. Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации».

16. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

17. Распоряжение Правительства Российской Федерации от 28.04.2023 № 1105-р.

Знание содержания данных нормативно-правовых актов позволит лицам, осуществляющим профилактическую деятельность, не только ознакомиться с ключевыми понятиями, требованиями, аспектами государственной политики и современными угрозами, стоящими перед российским обществом, но также поможет с планированием и подготовкой конкретных профилактических мероприятий. В частности, идеи по тематике мероприятий, в том числе аудиторных занятий, можно черпать в разделе III Доктрины информационной безопасности Российской Федерации, где обозначены ключевые угрозы в данной сфере, или в пункте 5 Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей, в котором перечислены данные ценности.

ВИДЫ И ФОРМЫ ПРОФИЛАКТИЧЕСКИХ МЕРОПРИЯТИЙ

Выбор конкретных видов и форм проведения профилактических мероприятий будет зависеть от особенностей субъекта и целевой аудитории. При этом крайне важно при выборе дидактических средств помнить о требованиях, предъявляемых к текстовой и аудиовизуальной продукции в зависимости от возраста потребителей. Таким образом, становится очевидным, что критический анализ растиражированного в СМИ и на различных интернет-платформах видеосюжета, в котором предположительно демонстрируются кадры принятой в одной из частных военных компаний казни за измену с использованием кувалды, будет в большей степени уместен в студенческой аудитории 18+, нежели среди восьмиклассников.

Следует отметить, что форм и видов профилактических мероприятий может быть множество, как и форм любой образовательной и воспитательной деятельности. Поэтому далее будут приведены лишь некоторые варианты. Основными видами при этом будут профилактические мероприятия в рамках учебного процесса и за его пределами, включая просветительскую деятельность, досуг, изготовление и распространение профилактического контента, волонтерство (рис. 6).



Рис. 6. Основные виды профилактических мероприятий

I. Профилактические мероприятия в рамках учебного процесса

1. Профилактический урок

Целевая аудитория: молодежь в возрасте 14—17 лет, учащиеся общеобразовательных и средних профессиональных образовательных учреждений.

Время проведения: 40—45 минут.

Цель: дать общие представления об информационной гигиене и ее правилах. Как вариант — рассмотреть лишь один из комплексов подобных правил, связанных, например, с умением верифицировать информацию.

Особенности: традиционный, легко организуемый в рамках образовательного процесса формат, позволяющий сформировать базовое представление об информационной гигиене и ее правилах. Важно при этом использовать аудиовизуальные материалы для обеспечения наглядности, так как разговор о современных методах информационного воздействия уместнее всего вести, когда сам педагог демонстрирует умение работы с информацией и информационными технологиями.

Одной из сложностей, которые могут возникнуть с проведением такого вида занятий, является возбуждение интереса аудитории, которая в рамках учебного процесса может ничего особенного не ждать от преподавателя, воспринимая урок как рутину. Здесь важно начать занятие с какого-то интересного случая или примера того, как знание или незнание основ информационной гигиены сказывается на жизни людей. Так, буквально недавно заблудившийся турист из Колорадо сутки не отвечал на звонки спасателей, так как они были с незнакомого номера¹ (рис. 7). К счастью, все обошлось, однако такая явно невротическая установка могла привести к трагедии. Все потому, что для человека, плохо владеющего навыками информационной гигиены, действительно любой незнакомый звонок становится проблемой и ввергает в состояние страха и растерянности, хотя в таких случаях важно не терять самообладание и помнить, что с незнакомого номера может звонить близкий человек, у которого сел или пропал телефон.



Рис. 7. Статья из газеты «Нью-Йорк Пост» о потерявшемся туристе, который не отвечал на звонки с незнакомых номеров

¹ Hiker lost for 24 hours ignored calls from rescuers because of unknown number // New York Post. 25.10.2021. URL: <https://nypost.com/2021/10/25/hiker-lost-for-24-hours-ignored-calls-from-rescuers-because-of-unknown-number/> (дата обращения: 15.05.2023).

2. Профилактическая лекция

Целевая аудитория: молодежь в возрасте 18—20 лет, студенты образовательных учреждений высшего образования.

Время проведения: 60—80 минут.

Цель: дать общие представления об информационной гигиене и ее правилах. Как вариант — рассмотреть лишь один из комплексов подобных правил, связанных, например, с умением верифицировать информацию.

Особенности: профилактическая лекция мало чем отличается от профилактического урока, за исключением того, что используемые в ней материалы могут относиться к категории 18+. Вместе с тем следует учитывать, что использование подобного контента даже в дидактических целях допустимо только тогда, когда это оправданно. Например, если некий случай действительно обладает высшей актуальностью или запрос на его критический анализ исходит от самих студентов. Кроме того, важно помнить, что в рамках проведения профилактической лекции обязательно следует оставлять время для вопросов аудитории.

Трудности здесь могут возникнуть те же, что и при проведении профилактического урока. Однако в данном случае, так как аудитория старше, для возбуждения интереса может использоваться какой-то более сложный и в каком-то смысле шокирующий случай, как, например, нашумевший во время пандемии коронавирусной инфекции COVID-19 флешмоб «Coronavirus challenge», направленный на молодежную аудиторию. Суть флешмоба состояла в том, чтобы продемонстрировать подписчикам отсутствие страха перед новой инфекцией, что заключалось в лизании на камеру различных предметов — от дверных ручек в публичных местах до общественных туалетов. Запустившая челендж девушка потом призналась, что перед тем, как сделать селфи с унитазом, она его тщательно продезинфицировала. Однако некритическое восприятие сделанного ею привело к тому, что молодые люди по всему миру начали по-настоящему лизать подобные предметы и попадать в больницы, как, например, блогер из Калифорнии¹. Появление первых жертв привело к тому, что социальные сети и видеохостинги стали блокировать подобный контент.

¹ California 'influencer' says he is in hospital with coronavirus just days after posting a video of himself licking a toilet bowl for a revolting TikTok challenge // Daily Mail. 25.03.2020. URL: <https://www.dailymail.co.uk/news/article-8150945/Influencer-hospital-coronavirus-just-days-posting-video-licking-toilet.html> (дата обращения: 15.05.2023).



Рис. 8. Видеосюжет о блогере из Калифорнии, который попал в больницу после участия в коронавирусном флешмобе

3. Деловая игра «Редакция»

Целевая аудитория: молодежь в возрасте 16—22 лет, как старшекласники, учащиеся в общеобразовательных учебных учреждениях, так и студенты учреждений высшего образования.

Время проведения: 80—90 минут.

Цель: развить навыки верификации информации.

Особенности: групповая работа, рассчитанная на 3—4 группы. В зависимости от аудитории это будут либо два урока, либо одна пара. Каждая группа — это редакция некоего СМИ. Ведущий — педагог — является «главным редактором» этого СМИ. Он дает группе от 5 до 10 новостей, которыми нужно наполнить новостную ленту вымышленного издания. Прежде чем опубликовать новость, «редакция» должна проверить предложенные «главным редактором» новости на соответствие фактам, установить их источники, чтобы сослаться на них, и подготовить на этой основе, в случае прохождения фактчекинга, собственные информационные материалы. Для усиления игрового момента каждая «редакция» может получить карточки с описанием того, какое именно «издание» она представляет — светскую хронику, спортивную газету, культурное обозрение, бульварную прессу, государственное СМИ и т. д. В конце занятия происходит презентация полученных результатов и их критический анализ членами конкурирующих редакций.

4. Деловая игра «Поймай меня, если сможешь!»

Целевая аудитория: молодежь в возрасте 15—22 лет, как старшекласники, учащиеся в общеобразовательных учебных учреждениях, так и студенты учреждений высшего образования.

Время проведения: 80—90 минут.

Цель: развить навыки верификации информации.

Особенности: групповая работа, рассчитанная на 3—4 группы. В зависимости от аудитории это будут либо два урока, либо одна пара. Каждая группа — это редакция некоего СМИ. Ведущий дает группе 3 новости, 3 фотографии, 3 аудиозаписи, 3 видеоролика и просит дать заключение о том, достоверная ли это информация. В конце занятия группы демонстрируют результаты и показывают, как они к ним пришли.

5. Деловая игра «Психологический портрет»

Целевая аудитория: молодежь в возрасте 18—22 лет, студенты учреждений высшего образования.

Время проведения: 80—90 минут.

Цель: развить навыки ответственного отношения к обеспечению защиты персональной информации.

Особенности: групповая работа, рассчитанная на 3—4 группы. В начале занятия выбирается ведущий — доброволец, психологический портрет которого будет описывать каждая группа. Если в группе добровольцев не будет, то таким может стать сам преподаватель. Ключевая задача — собрать из открытых источников — социальных сетей и разрозненной информации в Интернете — максимальное количество фактов о ведущем и на их основании сформировать его психологический портрет. В конце занятия каждая группа должна представить результат своего исследования и получить обратную связь от ведущего, а также рекомендации по обеспечению защиты персональных данных от преподавателя. Участники занятия должны понять, насколько много информации мы предоставляем на всеобщее обозрение и как легко эти данные могут быть собраны с различными целями.

6. Деловая игра «Экспертное бюро»

Целевая аудитория: молодежь в возрасте 18—22 лет, студенты учреждений высшего образования, преимущественно юридических, психологических, политологических, лингвистических направлений подготовки.

Время проведения: 80—90 минут.

Цель: развить навыки ответственного поведения в публичном пространстве.

Особенности: групповая работа, рассчитанная на 3—4 группы. Каждой группе — «экспертному бюро» — даются на экспертизу 2—3 высказывания в социальных сетях или популярных мессенджерах, это либо отдельные публикации (посты), либо комментарии. Задача группы определить, допустимы ли подобные высказывания в публичном пространстве, не нарушают ли они права и свободы других пользователей сети Интернет. В целях подготовки к занятию следует дать несколько ключевых нормативных правовых актов или выжимок из них для предварительного ознакомления, что позволит группам более профессионально аргументировать выводы, к которым они пришли.

II. Просветительские профилактические мероприятия

1. Публичная лекция

Целевая аудитория: молодежь в возрасте 14—35 лет. На самом деле формат отлично подходит для участников любого возраста.

Время проведения: 40—60 минут.

Цель: дать общие представления об информационной гигиене и ее правилах. Как вариант — рассмотреть лишь один из комплексов подобных правил, связанных, например, с умением верифицировать информацию.

Особенности: как правило, подобный формат реализуется в свободное от образовательного процесса время. При этом открытая лекция может проходить как в стенах образовательного учреждения (рис. 9), так и любого учреждения культуры, молодежной политики или вообще на независимых площадках. Например, такие мероприятия востребованы библиотеками, молодежными клубами, муниципальными культурно-досуговыми центрами. Если нет возможности напрямую контактировать с данными организациями, то можно обратиться к их учредителям — региональным органам государственной власти и местного самоуправления. Помощь в организации подобных открытых лекций могут оказывать также некоммерческие организации, в частности Российское общество «Знание». Для реализации этого вида профилактических мероприятий одним из самых важных требований является качественно подготовленная презентация. Также в конце выступления обязательно необходимо оставлять время на вопросы из аудитории.



Рис. 9. Публичная просветительская лекция «Критическое мышление и информационная гигиена», организованная Российским обществом «Знание»¹ и проходившая на базе МАУ СОШ № 59 г. Калининграда с интернет-трансляцией для 11 школ Калининградской области (всего очно и дистанционно в мероприятии приняли участие 180 учащихся)

¹ В регионе завершается всероссийская научно-просветительская акция «Ученые — в школы» // Правительство Калининградской области. 30.03.2023. URL: https://gov39.ru/press/328720/?sphrase_id=349922 (дата обращения: 15.05.2023).

2. Встречи с экспертами

Целевая аудитория: молодежь в возрасте 14—35 лет.

Время проведения: 40—60 минут.

Цель: дать представление о современных технологиях информационного воздействия и способах противостояния им.

Особенности: данный формат мероприятий предполагает предоставление молодым людям возможности в неформальной обстановке пообщаться с экспертами в области кибербезопасности или информационной гигиены. Как правило, это практики, работающие в органах государственной власти и местного самоуправления, в правоохранительных органах, в СМИ, а также в компаниях, занимающихся вопросами информационной безопасности. Одним из ярких примеров подобного формата являются мероприятия проекта «Открытый диалог», проходящие во всех регионах России по инициативе Министерства науки и высшего образования РФ.

III. Досуговые мероприятия

1. Квиз

Целевая аудитория: молодежь в возрасте 14—18 лет.

Время проведения: 90 минут.

Цель: в игровой форме познакомить с основными понятиями, правилами и наиболее интересными случаями в сфере информационной гигиены.

Особенности: квиз характеризуется динамичностью и разноплановым подбором заданий и включает в себя как ответы на текстовые вопросы, так и работу с изображением, видеороликами, аудиофрагментами. Все это прекрасно подходит для отработки всех основных навыков информационной гигиены.

2. Что? Где? Когда?

Целевая аудитория: молодежь в возрасте 18—35 лет.

Время проведения: 120 минут.

Цель: в игровой форме закрепить полученные знания в сфере информационной гигиены.

Особенности: тематические турниры по «Что? Где? Когда?» сегодня довольно популярны среди молодежи. Как правило, задаваемые вопросы рассчитаны непосредственно на знания аудитории и иногда на логику. То есть для подготовки к «Что? Где? Когда?» целесообразно порекомендовать литературу для изучения по теме. Материалом для вопросов может послужить законодательство в сфере защиты информации, конкретные случаи из литературы, новостей и популярной культуры.

3. Квест

Целевая аудитория: молодежь в возрасте 14—17 лет.

Время проведения: 90 минут.

Цель: в игровой форме закрепить полученные знания в сфере информационной гигиены.

Особенности: квест как наиболее динамичная из предложенных форм мероприятий прекрасно подходит для более юной аудитории, включает в себя и двигательную активность, и напряжение умственных способностей. Так, можно организовать квест «Хакеры», когда команда должна за короткое время решить ряд заданий, например по верификации контента, чтобы найти выход из комнаты.

IV. Изготовление и распространение профилактического контента

Целевая аудитория: молодежь в возрасте 14—35 лет.

Цель: изготовление полезного контента, позволяющего повысить информированность граждан о правилах информационной гигиены.

Особенности: в настоящий момент в сети Интернет появляется много полезных материалов, направленных на обеспечение безопасности взаимодействия индивидов с информационной средой. Распространение и использование в работе подобного контента также может оказывать помощь в проведении просветительской работы. Найти нужные материалы можно на сайтах как организаций, непосредственно занимающихся профилактикой негативных социальных явлений в молодежной среде (например, Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет, функционирующий на базе ФГАНУ НИИ «Спецвузавтоматика»), так и коммерческих организаций финансового сектора и сферы информационной безопасности, групп специалистов в области противодействия дезинформации (например, популярный телеграм-канал «Война с фейками», специализированные медиа — «Лапша медиа» и др.). Как правило, крупные организации и популярные интернет-ресурсы делают качественные просветительские информационные материалы (инфографика, видеоролики, видеолекции и уроки, памятки, разъясняющие карточки), которые хорошо воспринимаются целевой аудиторией.

V. Волонтерская деятельность

Целевая аудитория: молодежь в возрасте 14—35 лет.

Цель: помощь в организации и проведении профилактических мероприятий, распространении профилактического контента, выявлении противоправного контента в сети Интернет.

Особенности: привлечение волонтеров из числа молодежи позволяет повысить эффективность и нарастить масштаб профилактической работы, помочь молодым людям самим лучше усвоить основы информационной гигиены через помощь другим людям, например пенсионерам. Сегодня волонтеры есть почти в каждой школе и в каждом вузе. Их можно задействовать при проведении досуговых мероприятий, в качестве киберволонтеров и для распространения тематических информационных материалов.

ОБОБЩЕНИЕ ПОЛОЖИТЕЛЬНОГО ОПЫТА ФОРМИРОВАНИЯ ИНФОРМАЦИОННОЙ ГИГИЕНЫ В МОЛОДЕЖНОЙ СРЕДЕ

В настоящий момент в субъектах Российской Федерации только начинает разворачиваться деятельность по формированию умений и навыков информационной гигиены среди молодежи. В основном успешный опыт профилактики в данной сфере сконцентрирован в крупных общественных и коммерческих организациях, базирующихся в Москве и транслирующих свои наработки посредством сети Интернет. Сюда можно отнести инициативы и профилактический контент, направленные на детскую и молодежную аудиторию, Лиги безопасного Интернета или Всероссийского образовательного проекта в сфере информационных технологий «Урок цифры», который реализуется силами таких флагманов российской экономики, как «Яндекс», «Лаборатория Касперского», компания «1С», госкорпорация «Росатом» и «ВКонтакте», а также Академия искусственного интеллекта для школьников благотворительного фонда Сбера «Вклад в будущее». В качестве примера крупнейших региональных центров можно привести Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет, располагающийся в Ростове-на-Дону.

Если обобщать существующий на данный момент опыт регионов в сфере информационной гигиены, можно сделать вывод, что по большей части он складывается из изготовления и размещения полезного просветительского контента (памятки, видеолекции и видеоуроки, социальная реклама, буклеты, разъяснительные карточки), проведения профилактических занятий в рамках учебного процесса, добровольческих проектов, направленных на реализацию профилактических мероприятий во внеучебное время, публичных лекций, издания научных трудов.

I. Центральный федеральный округ

Москва

Ассоциация участников рынка интернет-индустрии «Лига безопасного Интернета»

Сайт: <https://ligainternet.ru/>

Лига собрала хорошую базу профилактического контента, включающую простые советы по безопасности, телефоны горячих линий и алгоритмы поведения, видеоуроки, просветительские акции и конкурсы. Сайт удобно структурирован по типам целевой аудитории — есть раздел для родителей, детей и подростков, педагогов (рис. 10). Информацию с сайта можно использовать как для проведения собственных профилактических мероприятий, так и для поиска тематических конкурсов и акций, в которых может принять участие молодежь из вашего региона.



Рис. 10. Информационные памятки для детей и подростков с сайта Лиги безопасного Интернета

Проект «Лапша медиа»

Сайт: <https://lapsha.media/>

Девиз проекта «Лапша медиа»: «Фейки — лапша XXI века. Мы ее снимаем». Инициаторы — АНО «Диалог Регионы». Сайт обладает удобным функционалом, здесь можно прочитать о разоблаченных фейках и подать информацию на проверку через анонимную форму. Материалы сайта не только полезны для ознакомления с тем, как ведется работа по созданию дезинформации и ее разоблачению, но и удобны для использования в дидактических целях, например при подготовке заданий для профилактических занятий с молодежью (рис. 11).

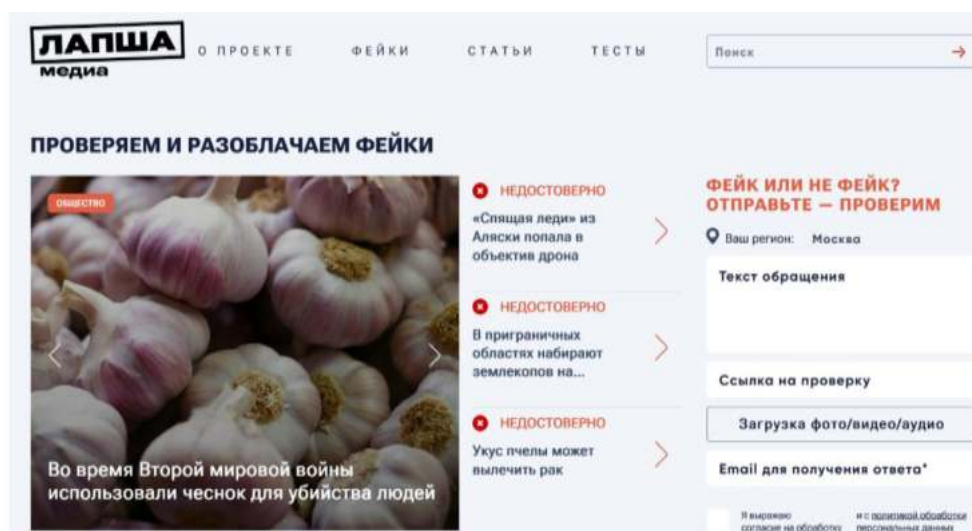


Рис. 11. Сайт интернет-проекта «Лапша медиа»

***Всероссийский образовательный проект
в сфере информационных технологий «Урок цифры»***

Сайт: <https://datalesson.ru/>

«Урок цифры» собрал лучшие практики информационной гигиены от флагманов российской экономики, таких как «Яндекс», «Лаборатория Касперского», компания «1С», госкорпорация «Росатом», «ВКонтакте», а также Академия искусственного интеллекта для школьников благотворительного фонда Сбера «Вклад в будущее». На сайте продумана навигация по материалам. В частности, можно выбрать не только тип интересующих материалов, но также отдельно посмотреть контент, предназначенный для родителей, детей или учителей.

Проект «Киберзож»

Сайт: <https://киберзож.рф/>

Совместный проект Минцифры России и ПАО «Ростелком» в сфере информационной гигиены. Позволяет изучить основные правила поведения в сети, в первую очередь касающиеся персональных данных и данных доступа к аккаунтам.

Telegram-канал «Война с фейками»

Адрес: t.me/warfakes

Один из самых популярных телеграм-каналов, которые занимаются разоблачением фейков. Каждый день здесь публикуются сообщения о подтвержденных фактах дезинформации, а также даются полезные советы по борьбе с аналогичными фейками. Как и у «Лапша медиа», в этом канале предусмотрена возможность направления информации на проверку.

Липецк

Видеокурс «Кибергигиена. Основы информационной безопасности»

Сайт: <https://stepik.org/course/125484/promo>

Видеокурс «Кибергигиена. Основы информационной безопасности» был разработан педагогом частного образовательного учреждения. Прохождение видеокурса бесплатно для всех желающих. Он размещен на одной из популярных российских образовательных онлайн-платформ. Как отмечает автор курса, программа строится на концепции подготовки учащихся к профессии киберследователя — профессии будущего, указанной в «Атласе новых профессий» и предполагающей проведение расследований киберпреступлений посредством поиска и обработки информации в интернет-пространстве. Курс стал ответом на возросшую потребность общества в технически грамотных специалистах, полностью отвечающих социальному заказу по подготовке квалифицированных кадров в области кибергигиены.

Тула

Памятка «Информационная гигиена»

Сайт: <https://azbyka.ru/zdorovie/informacionnaja-gigiena>

Памятка представляет интерес в силу того, что разработана психологом-консультантом Миссионерского отдела Тульской епархии РПЦ МП, и тем самым представляет точку зрения религиозного сообщества на проблему взаимодействия с информационной средой.

II. Северо-Западный федеральный округ

Калининград

Фейки: коммуникация, смыслы, ответственность

Золян С. Т., Пробст Н. А., Сладкевич Ж. Р., Тульчинский Г. Л. Фейки: коммуникация, смыслы, ответственность : монография. СПб. : Алетейя, 2021.

Монография «Фейки: коммуникация, смыслы, ответственность» стала, пожалуй, первой в истории отечественной науки попыткой систематического осмысления проблемы появления фейков (рис. 12). Книга представляет собой результат кропотливой работы ученых из БФУ им. И. Канта. Она может быть полезна как для повышения собственной квалификации в сфере информационной гигиены, так и для использования ее материалов в образовательном процессе.

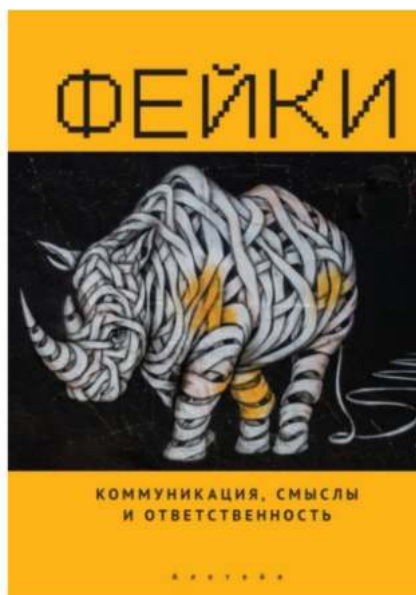


Рис. 12. Одна из первых в России монографий о фейках

Публичная лекция «Критическое мышление и информационная гигиена»

Сайт: https://gov39.ru/press/328720/?sphrase_id=349922

Публичная лекция «Критическое мышление и информационная гигиена» была организована Калининградским региональным отделением Российского общества «Знание» в одной из школ Калининграда в рамках всероссийской

акции «Ученые — в школу». Перед старшеклассниками выступал ученый-практик, старший научный сотрудник БФУ им. И. Канта, в том числе специализирующийся на проблемах связей с общественностью и информационной гигиене. Помимо возможности присутствовать на лекции очно у представителей образовательных учреждений других муниципальных образований региона была возможность посмотреть онлайн-трансляцию. Это хороший пример эффективной синергии усилий некоммерческих организаций, учреждений высшего и общего образования.

Санкт-Петербург

Игра-викторина «Правда-ложь»

Сайт: <http://www.tcmc.spb.ru/news/3408-ig911-03-2022>

В качестве примера того, как за пределами образовательного процесса студенты среднего профессионального образовательного учреждения сами могут организовать профилактическую работу, можно привести игру-викторину «Правда-ложь». Она была разработана и проведена членами Студенческого совета Санкт-Петербургского технического колледжа управления и коммерции в 2022 году. Игра была направлена на развитие навыков верификации. Подобные инициативы хороши тем, что исходят от самих студентов, поэтому воспринимаются другими учащимися лучше, чем что-то организованное администрацией учебного заведения.

Памятка по основам информационной гигиены

Сайт: <https://nsportal.ru/npo-spo/informatsionnaya-bezopasnost/library/2022/05/30/osnovy-informatsionnoy-gigieny-i>

Памятка «Основы информационной гигиены и информационной безопасности студентов» была разработана Санкт-Петербургским ГБПОУ «Пожарно-спасательный колледж «Санкт-Петербургский центр подготовки спасателей». Это пример довольно распространенного вида профилактического контента в образовательных учреждениях.

Вологда

Цикл лекций по информационной гигиене к Международному дню безопасного Интернета

Сайт: https://www.company.rt.ru/social/news/d466186/?sphrase_id=1812299/

При поддержке ПАО «Ростелеком» в городах Северо-Западного федерального округа прошла серия просветительских мероприятий для детей и подростков. Одним из партнеров акции стала Централизованная библиотечная система Вологды. Это хороший пример сотрудничества муниципальных учреждений и крупного российского телекоммуникационного бизнеса по формированию у подрастающего поколения базовых представлений о безопасном взаимодействии с информационной средой.

III. Южный федеральный округ

Ростов-на-Дону

Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет

Сайт: <https://ncpti.su/>

НЦПТИ был создан в 2012 году на базе НИИ «Спецвузавтоматика» с целью оказания информационно-аналитического, методического и технологического сопровождения деятельности ФОИВ, ОИВ субъектов Российской Федерации и образовательных организаций по противодействию идеологии терроризма и иным радикальным проявлениям в образовательной сфере и молодежной среде. Несмотря на то что профильными являются указанные выше цели, на сайте есть образовательный контент, направленный на формирование базовых представлений об информационной гигиене (рис. 13). Кроме того, НЦПТИ проводит тематические профилактические мероприятия, например Киберквиз.



Рис. 13. Разъясняющие карточки НЦПТИ

IV. Северо-Кавказский федеральный округ

Ессентуки

Программа подготовки «Информационная гигиена»

Сайт: [https://yesspi.ru/sveden/files/48._Informacionnaya_gigiena\(2\).pdf](https://yesspi.ru/sveden/files/48._Informacionnaya_gigiena(2).pdf)

В филиале ФБОУ ВО «Ставропольский государственный педагогический институт» в городе Ессентуки в 2020 году была разработана рабочая программа дисциплины «Информационная гигиена» для бакалавров по направлению подготовки «Психолого-педагогическое образование». Это довольно интересный опыт филиала регионального вуза. Как пишут авторы программы, целью освоения дисциплины «Информационная гигиена» является формирование

компетенций педагога-психолога в области обеспечения информационной безопасности, ответственного и безопасного поведения детей в современном информационном пространстве.

V. Приволжский федеральный округ

Казань

Проект «Информационная гигиена»

Сайт: <https://vk.com/informgigiena>

Как отмечают авторы проекта в своем сообществе в социальной сети «ВКонтакте», научно-образовательный проект «Информационная гигиена», разработанный кафедрой общей гигиены Казанского ГМУ Минздрава России, направлен на изучение закономерностей влияния информации на психическое, физическое и социальное благополучие человека, его работоспособность, продолжительность жизни, общественное здоровье социума. Также он представляет собой разработку гигиенических нормативов и мероприятий по повышению санитарной грамотности населения, оздоровлению окружающей информационной среды и экосистемы, оптимизации интеллектуальной и творческой деятельности человека. Многие мероприятия проекта реализуются с помощью волонтеров, привлеченных через всероссийскую платформу Добро.ru.

VI. Уральский федеральный округ

Нижний Тагил

Серия просветительских мероприятий по информационной гигиене

Сайт: https://tagilib.ru/for_prof/bibliotekaryu-dlya-raboty/program_and_project/?ELEMENT_ID=65433

Центральная городская библиотека Нижнего Тагила является хорошим примером того, как можно вести постоянную работу по формированию у молодежи компетенций в сфере информационной гигиены. Здесь регулярно проводятся разные формы профилактических мероприятий, благодаря чему достигается большой эффект.

VII. Сибирский федеральный округ

Омск

Международный конкурс «Информационная гигиена»

Сайт: <https://nic-snail.ru/calendar/-mezhdunarodnyy-konkurs-informatsionnaya-gigiena>

Международный конкурс «Информационная гигиена» — один из примеров просветительской деятельности небольшой региональной частной образовательной организации.

ОСНОВНЫЕ ВЫВОДЫ

Информационная гигиена — это совокупность компетенций, позволяющих обеспечить безопасное взаимодействие индивида и информационной среды. Вопреки расхожему мнению, информационная гигиена предполагает не только осознанное и ответственное потребление, но и осознанное и ответственное производство и распространение информации.

Важно понимать, что конкретных практических правил информационной гигиены может быть множество. В связи с этим целесообразно выделить три ключевые группы умений и навыков, которые составляют основу информационной гигиены, — это умения и навыки, касающиеся верификации информации, защиты персональных данных и данных доступа, а также поведения в публичном пространстве, которым стала сеть Интернет, особенно в контексте деанонимизации процесса онлайн-взаимодействия индивидов.

Выбор конкретных средств информационной гигиены будет варьироваться в зависимости от характера угроз, возникающих при взаимодействии индивидов и информационной среды. Причем данные угрозы быстро изменяются вместе с развитием технологий, что также нужно учитывать в процессе профилактики. Так, если еще недавно для выявления поддельного видео- и аудиоконтента достаточно было только обращать внимание на признаки применения технологий монтажа, то с развитием нейросетей и появлением технологии deepfake задача значительно усложнилась.

Вместе с тем следует помнить, что психика человека не может развиваться так же быстро, как новые технологии. Поэтому самую большую угрозу для взаимодействия с информационной средой представляют изъяны восприятия и мышления индивида. В связи с этим самым простым, универсальным, но при этом трудновыполнимым правилом информационной гигиены является формирование и постоянное совершенствование навыков критического восприятия и анализа информации.

Профилактическая работа в сфере информационной гигиены в молодежной среде может вестись как в рамках образовательного процесса, так и за его пределами. Сочетание этих двух подходов дает максимальную эффективность. Одно из главных требований при этом — постоянное повышение квалификации субъектов профилактики и обращение к опыту экспертного сообщества в данной отрасли, так как требуется постоянная актуализация знаний.

ЗАКЛЮЧЕНИЕ

Для достижения максимальной эффективности профилактическая деятельность в сфере информационной гигиены в молодежной среде должна проводиться комплексно и систематически.

Комплексность достигается комбинацией различных видов и форм профилактической работы, подбираемых соответственно характеру целевой аудитории и преследуемым задачам по формированию умений и навыков, направленных на противодействие конкретным угрозам взаимодействия индивида и информационной среды.

Если субъектом профилактики выступает лицо, которое уполномочено работать с молодежью в организациях сферы образования, спорта, культуры, молодежной и социальной политики, то систематичность достигается четким планированием, закреплением на административном уровне соответствующих функциональных обязанностей, установлением целевых показателей и мониторингом их достижения.

Если субъектом профилактики является родитель, то систематичность достигается за счет регулярности обращения к теме информационной гигиены, совместного разбора появляющихся в СМИ сообщений о новых угрозах в сфере взаимодействия индивидов и информационной среды, в частности о новых видах мошенничества или способах кибербуллинга.

Чтобы сохранять интерес молодежи к информационной гигиене, профилактические мероприятия в рамках учебного процесса должны обязательно дополняться досуговыми профилактическими мероприятиями, а также распространением полезного профилактического контента. Для более взрослой целевой аудитории большой потенциал имеет вовлечение в добровольческую деятельность, например в кибердружины или сообщества по разоблачению фейков.

Поскольку информационная гигиена во многом является ответом на стремительное развитие технологий, то обязательным требованием выступает как институциональное, так и самостоятельное повышение квалификации. Содействие в данном вопросе оказывают некоммерческие организации, экспертные площадки и сообщества, в большом количестве производящие сегодня качественный профилактический контент и проводящие просветительские мероприятия.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Балановский В. В. Роль информационной гигиены в условиях санитарно-эпидемиологических ограничительных мер // Современные технологии и подходы в юридической науке и образовании. Калининград: Издательство БФУ им. И. Канта, 2021. С. 360—367.
2. Берендеев М. В., Друкер М. В. Медиаэкология киберпространства как сфера безопасности потребления информации в российской интернет-среде // Вестник Волжского университета им. В. Н. Татищева. 2021. Т. 1, № 1 (34). С. 109—117.
3. Большаков А. М., Крутько В. Н., Кутепов Е. Н. и др. Информационные нагрузки как новый актуальный раздел гигиены детей и подростков // Гигиена и санитария. 2016. № 2. С. 173—177.
4. Бочкарева Е. В., Стренин Д. А. Теоретико-правовые аспекты кибербуллинга // Всероссийский криминологический журнал. 2021. Т. 15, № 1. С. 91—97.
5. Бухтияров И. В., Денисов Э. И., Еремин А. Л. Основы информационной гигиены: концепции и проблемы инноваций // Гигиена и санитария. 2014. № 4. С. 5—9.
6. Волчецкая Т. С., Авакьян М. В. Прикладные аспекты противодействия информационно-мировоззренческим угрозам в цифровом пространстве и особенности их профилактики // Актуальные проблемы российского права. 2021. Т. 16, № 6 (127). С. 194—201.
7. Волчецкая Т. С., Авакьян М. В., Осипова К. В. Криминологическая характеристика и профилактика скулшутинга и кибербуллинга в России и зарубежных странах // Всероссийский криминологический журнал. 2021. Т. 15, № 5. С. 578—591.
8. Волчецкая Т. С., Кот Е. А. Преступления, связанные с деятельностью «групп смерти»: проблемы выявления, расследования и профилактики. М. : Юрлитинформ, 2023.
9. Галяшина Е. И. Концепция информационной (мировоззренческой) безопасности в интернет-медиа в аспекте речеведческих экспертиз // Вестник Университета им. О. Е. Кутафина (МГЮА). 2020. № 6 (70). С. 33—43.
10. Гончарова А. А. Деструктивное влияние социальных сетей на взаимосвязь языка и мышления в контексте медиаэкологии // Вестник Томского государственного университета. 2019. № 444. С. 65—71.
11. Денисов Э. И. Роботы, искусственный интеллект, дополненная и виртуальная реальность: этические, правовые и гигиенические проблемы // Гигиена и санитария. 2019. Т. 98, № 1. С. 5—10.
12. Еремин А. Л. Информационная гигиена: современные подходы к гигиенической оценке контента и физических сигналов носителей информации // Гигиена и санитария. 2020. Т. 99, № 4. С. 351—355.

13. Еремин А. Л. Информационная и цифровая гигиена: учеб. пособие для вузов. СПб. : Лань, 2023.
14. Золян С. Т., Пробст Н. А., Сладкевич Ж. Р., Тульчинский Г. Л. Фейки: коммуникация, смыслы, ответственность. СПб. : Алетейя, 2021.
15. Кондрашкин А. В., Хломов К. Д. Девиантное поведение подростков и Интернет: изменение социальной ситуации // Психология. Журнал Высшей школы экономики. 2012. Т. 9, № 3. С. 102—113.
16. Ларина Е., Овчинский В. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. М. : Кн. мир, 2014.
17. Ломбина Т. Н., Мансуров В. А., Юрченко О. В. Проблемы чтения в новой цифровой реальности (на примере школьников). Ч. 2 // Социологическая наука и социальная практика. 2020. Т. 8, № 1. С. 93—105. doi: 10.19181/snsr.2020.8.1.7097.
18. Макаров С. Прекрасный, опасный, кибербезопасный мир. Все, что важно знать детям и взрослым о безопасности в интернете. М. : Ростелеком, 2022.
19. Медведев А. В., Лобанов К. Н., Крупенникова К. К. Роль педагогов в процессе формирования информационной гигиены несовершеннолетних // Образование и проблемы развития общества. 2022. № 2 (19). С. 43—48.
20. Молодцова И. А., Сливина Л. П., Максимова Е. А. Методологические основы информационной гигиены. Волгоград : Бланк, 2020.
21. Сапрыкин В. А. Деструктивное поведение молодежи в условиях информационной войны: колумбайн-вызовы и преодоления // Теория и практика общественного развития. 2019. № 1 (131). С. 18—21. doi: 10.24158/tipor.2019.1.2.
22. Стернин И. А., Шестернина А. М. Маркеры фейка в медиатекстах : рабочие материалы. Воронеж : ООО «РИТМ», 2020.

Балановский Валентин Валентинович

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
И МАТЕРИАЛЫ ПО ИНФОРМАЦИОННОЙ ГИГИЕНЕ
В МОЛОДЕЖНОЙ СРЕДЕ

Учебное электронное издание

Редактор *Е. Т. Иванова*
Компьютерная верстка *Е. В. Денисенко*

Дата выхода в свет 23.06.2023 г.
Формат 60×90 1/8. Усл. печ. л. 5,1