Областное государственное бюджетное

профессиональное образовательное учреждение

«Томский политехнический техникум»



Исследовательская работа

**«Основные правила безопасного использования Интернета»**

Автор: Р.В. Муравьев

Руководитель: О. В. Самсонова

Томск 2017

Содержание

Введение 4

Объекты угроз и их источники 5

Способы психологической защиты 6

Заключение 8

Приложение 9

Cписок литературы 10

**Цель работы:** Провести исследование по теме «Правила безопасного использования Интернета»

**Актуальность:** Информационное пространство оказывает беспрецедентное влияние на безопасность личности и общества. В XXI веке средства массовой информации присутствуют повсюду, превращая каждое событие в товар, делая из него зрелищный спектакль, часто напоминающий фильм ужасов, что, казалось бы, идет вразрез с их основной функцией — предоставлять аудитории объективную информацию о происходящем.

**Задачи:**

1. Рассмотреть угрозы информационной безопасности в обществе.
2. Определить способы психологической защиты.
3. Создать буклет-памятку интернет-пользователя.

**Методы:**

1. Изучение литературы.
2. Аналитическая деятельность.

**Введение**

В отношении человека государство должно обеспечивать информационно-психологическую безопасность.

Информационно-психологическая безопасность - состояние защищенности отдельных лиц и (или) групп лиц от негативных информационно-психологических воздействий и связанных с этим иных жизненно важных интересов личности, общества и государства в информационной сфере. Основными принципами обеспечения информационно-психологической безопасности являются:

- адекватность мер безопасности существующим угрозам;

- государственная монополия на разработку и производство специальных средств информационно-психологического воздействия;

- сочетание централизованного управления силами и средствами обеспечения информационно-психологической безопасности с передачей в соответствии с федеральным устройством России части полномочий в этой области органам государственной власти субъектов РФ и органам местного самоуправления;

- гласность и гражданский контроль за обеспечением информационно-психологической безопасности;

- обязательность участия общественных организаций в деятельности по обеспечению информационно-психологической безопасности.

**Объекты угроз и их источники**

К основным угрозам информационно-психологической безопасности относится возможность наступления негативных последствий для субъектов, подвергающихся информационно-психологическому воздействию, которые могут выражаться в следующих формах:

- причинение вреда здоровью человека;

- блокирование на неосознаваемом уровне свободы волеизъявления человека, искусственное привитие ему синдрома зависимости;

- утрата способности к политической, культурной, нравственной самоидентификации человека;

- манипуляция общественным сознанием, а также нарушении иных жизненно важных интересов личности, общества и государства. Источниками угроз информационно-психологической безопасности являются: 1) физические лица, обладающие природными способностями воздействия на психику людей; 2) разработка программных и технических средств; 3) религиозные и иные группы; 4) антропогенные зоны; 5) геопатогенные зоны.

**Объекты угроз**

Отдельные граждане, представляющие различные возрастные, социокультурные и национальные группы и слои общества;

Отдельные социальные группы и слои как компоненты социальной структуры общества (в том числе профессиональные, национально-этнические и др.);

Отдельные организации, группы и лица, конкретные представители органов государственной власти и управления, Вооруженных сил, органов правопорядка и безопасности, производственных, финансовых и других структур, осуществляющие деятельность, которая имеет или может иметь важные социальные последствия;

Общественные и политические организации, общественно-политические движения и партии;

Население страны в целом как социально-историческая общность людей, обладающая специфическими особенностями общественной психологии.

**Способы психологической защиты**

 Для обеспечения информационно-психологической безопасности личности можно рекомендовать различные способы психологической защиты. Они позволяют предотвратить или нейтрализовать негативное воздействие информации в различных ситуациях, контакт-коммуникационных и межличностных.

**Способ защиты 1-й: «Уход»**- увеличение дистанции, прерывание контакта, выход за пределы досягаемости информационного воздействия. Действия в различных информационных ситуациях могут быть такими:

* отключение определенных каналов СМИ (раздражающего канала телевидения, выход из Интернета и пр.), отказ от просмотра (прослушивания) конкретных теле-радиопрограмм;
* отказ от чтения некоторых газет, статей, рубрик и пр.;
* уход под различными предлогами с массовых зрелищных мероприятий: театра, концертного зала, кинотеатра и пр., митингов, собраний и др.;
* смена неприятной темы беседы, стремление не обострять межличностные отношения во время беседы.

В некоторых случаях защита может выразиться в более резких формах – **«изгнании»**или**«игнорировании»**.

При использовании способа **«изгнание»**средство или источник негативного информационного воздействия изгоняется (или вытесняется) из информационной среды (отказ от пользования телевизором или компьютером, отказ посещать театральные постановки или концерты и пр.).

**«Игнорирование»** предполагает невосприятие информации, которая затрудняет или препятствует определенной деятельности человека, может спровоцировать конфликт, вызвать негативные эмоции.

**Способ защиты 2-й: «Блокировка»**- контроль информационного воздействия, выставление психологических барьеров, ограждение психики от внешнего негативного информационного воздействия.  
Действия, выполняемые при «блокировке»:

* критическое восприятие информации;
* эмоциональное отчуждение (восприятие негативной информации «без эмоций»);
* увеличение межличностного пространства – «зоны общения» во время беседы;
* использование «психологических барьеров» (принижение источника информации, внутреннее осмеяние, развенчание авторитета, несерьезное восприятие информации, недоверие, настороженность, невнимательность, отвлечение и переключение внимания на другие объекты, не связанные с содержанием информационного воздействия и пр.).

**Способ защиты 3-й: «Управление»** - контроль процесса информационного воздействия, влияние на его характеристики и источник. Выполняемые действия:

* использование обратной связи (участие в опросах рейтинга популярности определенных каналов или программ телевидения, популярности периодических изданий и пр.);
* выражение в зрелищных мероприятиях своего отношения к происходящему (неодобрения, недовольства выступающими);
* использование при беседе принципа «своих не обижают», для чего продемонстрировать желание стать другом, членом одной общности; ослабить или дестабилизировать активность собеседника неожиданным отвлечением (например, сделать комплимент, высказать сочувствие) и др.

**Способ защиты 4-й: «Затаивание»** - контроль своей реакции на внешнее информационное воздействие. Выполняемые действия:

* отсрочка своих реакций, поспешных выводов и оценок, задержка или отказ от действий и поступков, вызываемых информационным воздействием (например, при нахождении в толпе, чтобы не поддаться «эффекту толпы»)
* маскировка, сокрытие чувств, проявлений эмоций и др.

 Умение человека в зависимости от ситуации воспользоваться тем или иным способом психологической защиты от негативного воздействия информации способствует формированию его информационной культуры, которая, в конечном счете, и обеспечит информационно-психологическую безопасность личности.

**Заключение**

В теории и практике информационной безопасности можно выделить два направления: защита информации и информационно-психологическая безопасность. Информационно-психологическая безопасность создает условия для обеспечения психического здоровья отдельной личности и населения страны в целом, надежного функционирования государственных и общественных институтов, а также формирования индивидуального, группового и массового сознания, нацеленного на прогрессивное развитие общества. Информационная безопасность – залог устойчивого развития экономики и общества.

Для безопасной работы в сети Интернет мной была разработана Памятка Интернет-пользователя, которая сможет помочь обеспечить свою безопасность в информационном пространстве (см. Приложение).

Приложение

**Список используемой литературы**

1. Доктрина информационной безопасности Российской Федерации. М., 2002.
2. Аносов В.Д., Стрельцов А.А.,  О Доктрине информационной безопасности Российской Федерации // Информационное общество. 1997. № 2–3. С. 3–9.
3. Аносов В.Д., Лепский В. Е., Стрельцов А. А.,  Проблемы обеспечения информационно-психологической безопасности // Информационное общество. 1997. № 4–6.
4. Арсентьев М.В.,  К вопросу о понятии «информационная безопасность»// Информационное общество. 1997. № 4–6.
5. Геополитика  и национальная безопасность: Словарь основных понятий и определений / М. И. Абдрахманов и др. М., 1998.
6. Емельянов Г.В., Стрельцов А.А.,  Информационная безопасность России: Учеб. пособие/ Под общ. ред. А. А. Прохожева. М., 1999. Ч. 1: Основные понятия и определения.
7. Емельянов Г.В., Стрельцов А.А.,  Проблемы обеспечения безопасности информационного общества // Информационное общество. 1999. № 2.