

ОГЛАВЛЕНИЕ:

Введение	3
Глава 1. Теоретические основы формирования информационной безопасности личности	8
1.1 Понятие информационной безопасности личности	8
1.2 Социальные сети как новая угроза безопасности личности	20
1.3 Информационные угрозы личности в сетевой коммуникации (информационные опасности сетевых коммуникаций)	22
Выводы по первой главе	33
Глава 2. Методика формирования информационной безопасности личности у студентов ПОО (на базе ОзТК)	35
2.1. Методы формирования информационной безопасности личности у студентов ПОО (на базе ОзТК)	35
2.2. Опытно – практическая работа по формированию информационной безопасности личности у студентов ПОО (на базе ОзТК). Анализ опытнo – практической работы	40
2.3. Разработка рекомендаций	49
Выводы по второй главе	51
Заключение	52
Список использованных источников	56
Приложение1	60

ВВЕДЕНИЕ

Актуальность темы исследования. За последние годы огромную популярность приобрели сайты социальных сетей. Они представляют собой компьютерные технологии, получившие значительное распространение в мире Интернета. Отметим, что самым распространенным контингентом пользователей социальных сетей, страдающих психологической зависимостью, являются молодые люди, ведь социальная сеть является одним из факторов их социализации. Наибольшей популярностью пользуются такие социальные сети, как Инстаграм, Одноклассники, ВКонтакте, Мой Мир.

На сегодняшний день ученые всерьез задумались над проблемой интернет-зависимости молодежи от социальных сетей. Эту «болезнь» изучают такие ученые, как Джеймс Барсонс, А. Ю. Мухарлямова, Г. В. Нестерова, А. И. Сидоров, М. А. Шаталина, К. Янг и другие. Данная проблема вызывает серьезный научный интерес в сообществе ученых, однако вопросы, касающиеся данной области, недостаточно изучены и описаны в учебниках и другой научной литературе.

Учеными установлено, что социальные сети имеют огромный потенциал – как положительный, так и отрицательный, что вызывает острую необходимость в осуществлении общественного контроля за поведением отдельных индивидов.

Прежде всего подчеркнем, что основной функцией социальных сетей является обеспечение поддержания взаимных связей между людьми, даже на расстоянии.

С помощью социальных сетей каждый человек может легко общаться не только с друзьями, коллегами, родными, но и заводить новые знакомства, и более того, найти людей, с которыми человек по различным причинам потерял связь. Имеется статистика о том, сколько семей было создано благодаря знакомству именно в социальных сетях. Сегодня для молодежи социальные сети – это самый распространенный вид знакомства и общения. Также одним из положительных

влияний социальных сетей является возможность личности самореализоваться в глазах друзей и знакомых.

Человек может без труда и в кратчайшие сроки найти своих единомышленников из различных частей света. Во всемирной паутине можно найти большое количество различных групп, в которых люди могут обмениваться накопленным опытом или просто своими взглядами на жизнь. Кроме того, социальные сети являются огромным хранилищем различной информации, для поиска которой не нужно прилагать огромных усилий (видео, музыкальные файлы, фото), среди которых можно найти редкие или нужные экземпляры.

Также погружение в мир социальных контактов во многом способно положительно повлиять на нервную систему, человек получает позитивные эмоции от общения, положительного результата поиска давно забытого человека, потребления познавательного и развлекательного контента.

Что же касается отрицательного влияния социальных сетей на развитие личности, то можно отметить наиболее распространенную проблему – зависимость от виртуального мира, что в дальнейшем может спровоцировать неврозы и депрессию.

Информационная безопасность личности — это состояние защищённости жизненно важных интересов человека в информационной сфере от внутренних и внешних угроз. Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещённой законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Понятие «информационная безопасность личности» может рассматриваться в узком и широком смысле:

- В узком смысле — это состояние, при котором отсутствует возможность причинения человеку вреда сведениями из внешнего мира.

- В широком смысле — это обеспечиваемое государством, общественными и иными организациями или отдельными гражданами состояние защищённости от внешних и внутренних угроз конституционных прав человека и гражданина на поиск, получение, производство, распространение информации, на неприкосновенность информации о частной жизни, а также психики человека от деструктивного воздействия информации.

Систему информационной безопасности личности образуют:

- Информационно-правовая безопасность — состояние защищённости права человека искать, получать, передавать, производить и распространять информацию, а также права на неприкосновенность информации о частной жизни.

- Информационно-психологическая безопасность — состояние защищённости человека от негативных информационных воздействий и внедрения деструктивной информации в сознание или подсознание индивида, позволяющих специальными средствами и методами воздействовать на психику и определять поведение.

Понятие «информационная безопасность личности» закреплено в нормативных документах:

- Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. №646) — определяет информационную безопасность как состояние защищённости личности от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина.

- Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» — фиксирует базовые нормы для всей системы информационного законодательства, в том числе правового обеспечения информационной безопасности;

В настоящее время существует довольно большое количество работ, посвященных формированию информационной безопасности личности в социальных сетях у студентов профессиональной образовательной организации-

это научные и научно-практические статьи, монографии, диссертационные исследования, но степень научной разработанности темы остается невысокой, актуальной из-за динамично повышающейся вовлеченности в различные сетевые форматы взаимодействия.

Объект исследования: взаимодействие студентов профессиональной образовательной организации в социальных сетях.

Предмет исследования: формирование информационной безопасности личности в социальных сетях у студентов профессиональной образовательной организации в процессе их взаимодействия в социальных сетях.

Цель исследования: разработать и апробировать программу формирования информационной безопасности личности в социальных сетях для студентов профессиональной образовательной организации на основе диагностики их актуальных практик и рисков в цифровой среде.

Руководствуясь основными целями исследования, были поставлены следующие **задачи исследования:**

1. Проанализировать теоретические подходы к проблеме информационной безопасности личности в социальных сетях в психолого-педагогической литературе.

2. Провести диагностику текущего уровня информационной безопасности и выявить типичные модели рискованного поведения студентов ПОО в социальных сетях (на базе ОзТК)

3. Определить педагогические условия и ресурсы образовательной организации для формирования информационной безопасности студентов.

4. Разработать и апробировать программу формирования информационной безопасности личности в социальных сетях для студентов ПОО.

5. Оценить эффективность апробированной программы и сформулировать методические рекомендации для педагогического коллектива.

Методологическую основу работы составляют как общенаучный диалектический метод познания, так и частно - научные методы: исторический, формально-логический, статистический и другие.

Теоретическая значимость работы заключается в том, что сформулированные в ней положения развивают и уточняют педагогические условия формирования информационной безопасности личности в социальных сетях у студентов профессиональной образовательной организации.

Практическая значимость состоит в возможности использования методических рекомендаций по формированию информационной безопасности личности в социальных сетях у студентов профессиональной образовательной организации в иных образовательных организациях.

Эмпирическую базу исследования составляют анализ научно-методической литературы, материалы опроса, анкетирования, обобщение педагогического опыта.

Структура работы обусловлена поставленными целью и задачами настоящего исследования. Работа состоит из введения, двух глав, включающих шесть параграфов, заключения, списка использованных источников и литературы.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ФОРМИРОВАНИЯ ЛИЧНОСТИ

1.1 Понятие информационной безопасности личности

Современное эффективное развитие России невозможно без интеграции в глобальное информационное общество. Информационное общество — это «специфическая форма социальной организации, в которой новые технологии генерирования, обработки и передачи информации стали фундаментальными источниками производительности и власти».

Наблюдаемые процессы интеграции и унификации оказывают заметное влияние на информационные отношения¹. Под воздействием глобализации информационные потоки выходят за рамки национальных и интегрируются в мировое информационное пространство, чему в значительной степени способствует совершенствование в ходе информационной революции коммуникационных систем и способов использования космического пространства для передачи информации.

Хартия глобального информационного общества² прямо утверждает, что «информационно-коммуникационные технологии (ИТ) являются одним из наиболее важных факторов, влияющих на формирование общества XXI века. Их революционное воздействие касается образа жизни людей, их образования и работы, а также взаимодействия правительства и гражданского общества».

Целью формирования и развития информационного общества в Российской Федерации является повышение качества жизни граждан, обеспечение конкурентоспособности России, развитие экономической, социально-политической, культурной и духовной сфер жизни общества,

¹ Кастель Г. Информационная эпоха: экономика, общество и культура[Текст] / Кастель Г.. М. : ГУ ВШЭ, 2018. С. 29.

² Чернов А. А. Становление глобального информационного общества: проблемы и перспективы[Текст] / А. А.Чернов. М., 2020. С. 14—15.

совершенствование системы государственного управления на основе использования информационных и телекоммуникационных технологий.

К числу основных задач, требующих решения для достижения поставленной цели, Стратегия развития информационного общества в Российской Федерации (утв. Президентом РФ 7 февраля 2008 г. № Пр-212), в частности, относит совершенствование системы государственных гарантий конституционных прав человека и гражданина в информационной сфере.

Информационная сфера, в соответствии с Доктриной информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) (далее — Доктрина информационной безопасности), представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

Статья 2 Конституции РФ устанавливает, что признание, соблюдение и защита прав и свобод человека и гражданина — обязанность государства. Гарантии прав и свобод человека и гражданина включают условия, средства, меры, направленные на обеспечение осуществления, охрану и защиту этих прав и свобод³.

К конституционным правам человека и гражданина в информационной сфере традиционно относят:

- право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ч. 4 ст. 29);
- запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия (ч. 1 ст. 24);
- предоставление каждому возможности ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, которую

³ Варакин А. В. Влияние социальных сетей на формирование ценностных ориентиров современной молодежи [Текст] / А. В. Варакин // Преподаватель XXI век. 2016. № 2. С. 205–212.

должны обеспечить органы государственной власти и органы местного самоуправления, их должностные лица, если иное не предусмотрено законом (ч. 2 ст. 24);

— право на достоверную информацию о состоянии окружающей среды (ст. 42). Следует также учитывать положения ч. 1 ст. 55 Конституции РФ о том, что перечисление в Конституции РФ основных прав и свобод не должно толковаться как отрицание или умаление других общепризнанных прав и свобод человека и гражданина. Кроме того, в ч. 4 ст. 15 Конституции РФ говорится о том, что общепризнанные принципы и нормы международного права и международные договоры Российской Федерации являются составной частью ее правовой системы. К таким международно-правовым нормам можно отнести прежде всего Всеобщую декларацию прав человека (утв. Генеральной Ассамблеей ООН 10 декабря 1948 г.), в которой впервые были отражены информационные права и свободы, и Конвенцию Совета Европы о защите прав человека и основных свобод (Рим, 4 ноября 1950 г.), которая развивает положения, закрепляющие информационные права и свободы.

Одной из мер обеспечения осуществления прав и свобод человека и гражданина в информационной сфере является поддержание необходимого уровня информационной безопасности и непосредственно такой ее составляющей, как информационная безопасность личности.

В то же время существуют значительные юридические препятствия в обеспечении информационной безопасности личности, к которым следует, на наш взгляд, отнести неопределенность (неясность) содержания норм права, регулирующих отношения в информационной сфере. Наличие препятствий-пробелов в законодательстве выражается, например, в отсутствии законодательно закрепленного определения ряда важнейших правовых категорий⁴.

⁴ Реснянская М. А., Кузьмина С. В. Влияние социальных сетей на мировоззрение студентов [Текст] / М. А. Реснянская, С. В. Кузьмина // Молодой ученый. 2016. № 9.4. С. 61–63.

Так, в настоящее время в законодательстве отсутствует понятие «безопасность». Закон РФ от 5 марта 1992 года № 2446-1 «О безопасности» определял безопасность как состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. Этот Закон утратил силу в связи с принятием Федерального закона от 28 декабря 2010 г. № 390-ФЗ «О безопасности», который определяет основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством Российской Федерации полномочия и функции федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления в области безопасности, а также статус Совета Безопасности Российской Федерации и при этом самого понятия «безопасность» не содержит.

В Стратегии национальной безопасности Российской Федерации до 2020 года (утв. Указом Президента РФ от 12.05.2009 № 537) (далее — Стратегия национальной безопасности) понятие «национальная безопасность» определяется как состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства. Однако закрепление этого определения в Стратегии национальной безопасности нельзя считать полноценной заменой понятия «безопасность» в федеральном законе. Юридический статус такого документа ниже, чем закон. Данное обстоятельство отрицательно влияет на правоприменение⁵.

⁵ Саенко Л. А., Егоров М. В. Сетевое общество в контексте современных социальных трансформаций[Текст] / Л. А.Саенко, М. В. Егоров // Дискуссия. 2018. № 7 (48). С. 88–93.

Немногим лучше выглядит ситуация с определением понятия «информация».

Происхождение слова «информация» относится к латинскому *informatio*, в переводе обозначающего «сведение, разъяснение, ознакомление». Значительное влияние на процесс наполнения термина «информация» дополнительным содержанием, которое отражало прежде всего ее коммуникативные свойства, оказали широкое внедрение в жизнь информационных технологий и развитие науки кибернетики.

В словаре С. И. Ожегова «информация» определяется как сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальными устройствами⁶.

В связи с необходимостью правового регулирования отношений в информационной сфере отечественный законодатель предпринял первую попытку дать определение понятия «информация» в Федеральном законе от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информации». Под информацией указанный Закон понимал сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их предоставления. Однако, как отмечается правоведами, такое определение не содержало основных признаков информации, выражающих ее юридическую сущность⁷.

Принятие Федерального закона от 7 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Закон об информации) взамен прежнего, по мнению правоведов, позволило приблизить законодательство Российской Федерации к международной практике регулирования информационных технологий; унифицировать как с понятийной, так и содержательной точки зрения принципы и правила регулирования информационных отношений; заложить эффективную правовую

⁶ Ожегов С. И. Словарь русского языка : Около 57 000 слов[Текст] / С. И. Ожегов / под ред. д-ра филол. наук, проф. Н. Ю. Шведовой. 14-е изд., стереотип. М. : Рус. яз., 1982. С. 224.

⁷ Кузьмин В. П. Понятие и юридическая сущность информации и пути формирования информационного общества в России[Текст] / В. П. Кузьмин // Информационное право. 2019. № 2. С. 3.

основу создания и эксплуатации государственных и иных информационных систем; законодательно закрепить принципы использования информационно-телекоммуникационных сетей, в том числе при международном информационном обмене⁸.

Согласно положениям действующего законодательства под информацией понимаются любые сведения (сообщения, данные) независимо от формы их представления. Как можно отметить, понятие «информация» в новом Законе было представлено в более общем виде. Считается, что такое определение лучше охватывает юридический характер данного термина, по сравнению с ранее действовавшим. В то же время вторая попытка законодателя признается вновь неудачной и высказываются справедливые опасения о том, что предложенное слишком абстрактное определение может стать причиной неточных толкований⁹.

Довольно тесно с понятием «информация» связано понятие «сведения», которые понимаются как познания в какой-нибудь области, известия, сообщения, знания, представление о чем-нибудь. В определении, предлагаемом законодателем, информация выступает как обобщающая величина различных сведений (сообщений, данных). В таком случае определить грань перехода отдельных сведений в полноценную информацию сложно, и, по-видимому, опираться следует на категорию их достаточности для возможности на их основе прийти к определенному умозаключению.

Рассмотренные выше понятия «безопасность» и «информация» являются основополагающими для определения категории «информационная безопасность», которая активно изучается правоведами.

А. А. Малюк понимает информационную безопасность как состояние рассматриваемой системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних

⁸ Просвирнин В. Г., Просвирнин Ю. Г. Понятие и правовые основы информационных технологий [Текст] / В. Г. Просвирнин, Ю. Г. Просвирнин // Юридические записки. 2019. № 2 (25). С. 151.

⁹ Зейналов З. З. Проблемы определения информации как объекта информационных правоотношений [Текст] / З. З. Зейналов // Информационное право. 2019. № 1. С. 10.

информационных угроз, а с другой — ее функционирование не создает информационных угроз для элементов самой системы и внешней среды¹⁰.

Т. В. Закупень отмечает, что информационная безопасность представляет собой социальное, а не чисто техническое явление. Ее нельзя отождествлять с применением специальных технических средств и методов для защиты информации от несанкционированного доступа, похищения, уничтожения и т.д.¹¹

А. В. Еркин дает определение информационной безопасности для информационного общества: «это состояние рассматриваемой системы управления, при котором ее информационная инфраструктура не дестабилизируется под воздействием внешних и внутренних угроз; восприятие результата ее деятельности во внешнем окружении является объективным»¹².

По мнению Л. И. Шершнева, «информационная безопасность — способность государства, общества, социальной группы, личности обеспечить с определенной вероятностью достаточные и защищенные информационные ресурсы и информационные потоки для поддержания жизнедеятельности, устойчивого функционирования и развития, противостоять информационным опасностям и угрозам, негативным информационным воздействиям на индивидуальное и общественное сознание и психику людей, а также на компьютерные сети и другие технические источники информации, вырабатывать личностные и групповые навыки и умения безопасного поведения, поддерживать постоянную готовность к адекватным мерам в информационном противоборстве, кем бы оно ни было навязано»¹³

Доктрина информационной безопасности определяет информационную безопасность Российской Федерации как состояние защищенности ее

¹⁰ Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации : учеб. пособие для вузов[Текст] / А. А.Малюк. М. : Горячая линия — Телеком, 2018. С.56.

¹¹ Еркин А. В. Понятия «информация» и «информационная безопасность»: от индустриального общества к информационному[Текст] / А. В. Еркин // Информационное общество. 2020. № 1. С. 73.

¹² Закупень Т. В. Понятие и сущность информационной безопасности и ее место в системе обеспечения национальной безопасности РФ[Текст] / Т. В. Закупень // Информационные ресурсы России. 2021. № 4. С. 28—34.

¹³ Шершнева Л. И. Информационная безопасность России[Текст] / Л. И. Шершнева // Безопасность. 2021. № 11—12. С. 49—50.

национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. В приведенном определении, на наш взгляд, прослеживается четкая связь с определением «безопасности», которое содержал Закон РФ «О безопасности», и прямо выводится из него с выделением специфики регулируемых правоотношений.

Информационная безопасность является одной из составляющих национальной безопасности Российской Федерации, она оказывает влияние на защищенность национальных интересов Российской Федерации в различных сферах жизнедеятельности общества и государства.

Согласно Стратегии национальной безопасности, национальные интересы Российской Федерации — это совокупность внутренних и внешних потребностей государства в обеспечении защищенности и устойчивого развития личности, общества и государства. На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Разделение в Доктрине информационной безопасности национальных интересов в информационной сфере на такие элементы, как интересы личности, общества и государства, можно принимать с определенной долей условности. Употребление термина «личность» в данном случае является несомненным синонимом понятия «человек», используемого в нормативных правовых актах. Тем более что сама Доктрина утверждает, что интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность. Таким образом, реализация прав каждого человека в информационной сфере признается одной из составляющих информационной безопасности России. Поэтому мы считаем верным

выделение А. А. Стрельцовым таких составляющих информационной безопасности России, как «информационная безопасность человека, общества и государства»¹⁴

Закон Российской Федерации «О безопасности» содержал определение понятия «жизненно важные интересы», под которыми понималась совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства. Некоторые авторы предпринимали попытки раскрыть содержание указанного понятия применительно к интересам личности в информационной сфере¹⁵. Однако, при всем уважении к институтам прав на поиск, получение, производство и распространение информации, на неприкосновенность частной жизни, на защиту прав на объекты интеллектуальной собственности, считаем отнесение их к «жизненно важным интересам» личности преувеличением.

По мнению С. В. Иванова, информационная безопасность личности — это «состояние высокой степени защищенности личности, при котором гарантируется реализация ее прав и свобод в информационной сфере, и максимально снижен риск негативного воздействия на нее внутренних и внешних угроз»¹⁶.

Г. Г. Гафарова и В. В. Смелянская более критичны в подходе к размерам негативного воздействия и считают, что информационная безопасность характеризуется отсутствием угрозы причинения вреда информации, которой владеет личность и угрозы нанесения вреда личности информацией¹⁷.

Если считать, что информационная безопасность — идеальная цель, на достижение которой направлены меры, предпринимаемые субъектами ее

¹⁴ Стрельцов А. А. Обеспечение информационной безопасности России. Теоретические и методологические основы [Текст] / А. А. Стрельцов / под ред. В. А. Садовниченко и В. П. Шерстюка М. : МНЦМО, 2019. С. 52—57.

¹⁵ Ковалева Н. Н. Информационное право России : учеб. пособие [Текст] / Н. Н. Ковалева. М. : Дашков и Ко, 2017. С. 109.

¹⁶ Иванов С. В. Правовое регулирование информационной безопасности личности в Российской Федерации [Текст] / С. В. Иванов // Вестник Екатеринбургского института. № 1 (25). 2019. С. 50.

¹⁷ Гафарова Г. Г., Смелянская В. В. Информационная безопасность личности [Текст] / Г. Г. Гафарова, В. В. Смелянская // Безопасность личности: состояние и возможности обеспечения : материалы междунар. науч.-практ. конференции 10—11 мая 2012 года. Ереван, Пенза, Колин : Социосфера, 2019. С. 57.

обеспечения, то подход Г. Г. Гафаровой и В. В. Смелянской следует признать более приемлемым. Введение С. В. Ивановым такого критерия информационной безопасности, как «максимальное снижение риска негативного воздействия», может быть использовано в качестве установления уровней информационной безопасности в каком-либо конкретном случае.

Нельзя считать удачным, на наш взгляд, определение понятия «информационная безопасность личности» как «состояния и условий жизнедеятельности личности, при которых реализуются ее информационные права и сво-боды»¹⁶. Очевидно, что реализация информационных прав и свобод личности в некоторой степени может происходить при негативных обстоятельствах, прямо или косвенно угрожающих ее интересам. Считаем, что в таких условиях можно вести речь только об уровне обеспечения информационной безопасности личности¹⁸.

Ближайшим по значению к информационной безопасности личности определением, закрепленным в законодательстве, следует считать понятие «информационная безопасность детей», которое содержит Федеральный закон от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (далее — ФЗ № 436).

Согласно ч. 1 ст. 54 Семейного кодекса РФ, ребенком признается лицо, не достигшее возраста 18 лет (совершеннолетия). Очевидно, что возрастной критерий для человека является относительной величиной для установления полной дееспособности, что подтверждает, например, институт эмансипации несовершеннолетних. Именно поэтому нормы, устанавливаемые в ФЗ № 436, должны являться основой для правотворчества при регулировании отношений, обеспечивающих информационную безопасность личности.

Согласно ст. 2 ФЗ № 436 «информационная безопасность детей» представляет собой состояние защищенности, при котором отсутствует риск,

¹⁸ Григорьев Ю. Г. Сотовая связь: радиобиологические проблемы и оценка опасности. Радиационная биология. Радиоэкология[Текст] / Ю. Г.Григорьев. 2019. № 5. С.56.

связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию. Таким образом, законодатель также признает безопасностью не максимальное снижение риска, а его отсутствие.

На основе проведенного анализа можно сформулировать правовое определение информационной безопасности личности как состояния защищенности, при котором отсутствует риск, связанный с причинением информацией вреда здоровью и (или) физическому, психическому, духовному, нравственному развитию человека

Отметим также, что в содержании информационной безопасности личности отдельные исследователи выделяют:

— информационно-техническая безопасность, под которой понимается «защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры»¹⁹;

— информационно-идеологическая безопасность, определяемая как защищенность личности от преднамеренного или непреднамеренного информационного воздействия, имеющего результатом нарушение прав и свобод в области создания, потребления и распространения информации, пользования информационной инфраструктурой и ресурсами, противоречащего нравственным и этическим нормам, оказывающего деструктивное воздействие на личность, имеющего негласный (внечувственный, неосознанный) характер, внедряющего в общественное сознание антисоциальные установки;

— информационно-психологическая безопасность личности как «состояние защищенности ее психики от действия многообразных информационных факторов, препятствующих или затрудняющих формирование и функционирование адекватной информационно-

¹⁹ Галатенко В. А. Информационная безопасность [Текст] / В. А. Галатенко // Открытые системы. 2021. № 1 (15). С. 38—43.

ориентировочной основы социального поведения человека (и в целом жизнедеятельности в обществе), а также адекватной системы его субъективных (личностных, субъективно-личностных) отношений к окружающему миру и самому себе»;

— информационно-правовая безопасность личности как «состояние защищенности права человека искать, получать, передавать, производить и распространять информацию, а также права на неприкосновенность информации о частной жизни».

Не останавливаясь подробно на различиях в трактовке приведенных выше элементов, отметим, что попытки их теоретического обоснования являются безусловным доказательством сложности и многоаспектности правовой категории «информационная безопасность личности». Предложенное выше правовое определение понятия «информационная безопасность личности», на наш взгляд, создаст необходимые предпосылки для дальнейшей теоретической разработки и законодательного закрепления ее элементов. Принятие отечественного кодифицированного нормативного акта, в котором мог бы присутствовать специальный раздел, включающий нормы, посвященные обеспечению таких составляющих информационной безопасности, как информационная безопасность личности, общества и государства, по нашему мнению, способствовало бы преодолению существующих юридических препятствий. Информационная безопасность личности — это состояние защищенности жизненно важных интересов человека в информационной сфере от внутренних и внешних угроз. Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Таким образом, считаем, информационная безопасность как состояние рассматриваемой системы, при котором она, с одной стороны, способна

противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой — ее функционирование не создает информационных угроз для элементов самой системы и внешней среды.

1.2 Социальные сети как новая угроза безопасности личности

Интернет прочно вошёл в жизнь современной молодёжи. Сегодня многие пользователи уделяют огромное значение популярным социальным сетям. Подобные веб-сайты имеют много сторонников, но и немало противников. Каждые, из которых приводят массу доводов в пользу своей точки зрения²⁰. Особенно виртуальный мир является на данный момент привлекательным в глазах молодых людей. В социальных сетях они могут не только делиться своими эмоциями и переживаниями, вступать в группы по интересам, но также здесь есть возможность самовыражения и знакомства с новыми людьми и т.д. Также стоит отметить, что важной особенностью посещения социальных сообществ молодыми людьми является общение с друзьями, знакомыми и родственниками; знакомство со своими сверстниками, потребность в самовыражении собственной личности. Пользователи находят здесь моральную отдушину, закрываясь от внешнего мира. Например, в настоящее время в России за 2015 год социальную сеть «Вконтакте» ежедневно посещает более 54,6 млн. пользователей, «Одноклассники» – 40 млн. пользователей, в «Facebook» заходят 24,2 млн. человек.

Положительное влияние социальных сетей на студентов

Прошло то время, когда социальные сети были местом, где люди только общаются и знакомятся. Сейчас пользователи социальных сетей обмениваются информацией, получают новые знания и даже строят бизнес. Студентам соцсети тоже дают много преимуществ²¹:

²⁰ Хараш А. У. Психология одиночества[Текст] / А. У. Хараш // Педология. 2000. № 4 (ноябрь). С. 7–16.

²¹ Григорьев Ю. Г. Эмоциональный стресс и электромагнитные поля. Ежегодник Российского Национального Комитета по защите от неионизирующих излучений[Текст] / Ю. Г. Григорьев. М.: Изд-во РУДН, 2021. С.46.

1. С помощью социальных сетей студенты общаются с единомышленниками из разных стран и городов. Так молодые люди расширяют свой круг общения и находят новых друзей и знакомых. А студентам-интровертам социальные сети помогают найти друзей и уйти от одиночества.

2. Благодаря социальным сетям студенты повышают свой уровень знаний по разным предметам и быстро ищут нужную информацию. В соцсетях можно подписаться на группы по интересам и быстро получать нужную и интересную информацию.

3. Соцсети помогают студентам в учебе. С помощью социальных сетей учащиеся обмениваются конспектами, электронными пособиями, лабораторными работами и другой полезной для учебного процесса информацией.

4. Социальные сети помогают студентам подрабатывать удаленно. Некоторые учащиеся создают в соцсетях экспертные блоги, в которых делятся разного рода полезной информацией. Этим они могут заработать деньги и даже начать строить свою карьеру.

Отрицательное влияние социальных сетей на студентов

Несмотря на все плюсы соцсетей, у них есть и свои недостатки:

1. Главная опасность социальных сетей для молодежи — это реклама и пропаганда наркотиков и алкоголя. Как правило, эти пагубные пристрастия подаются в соцсетях в привлекательном и безопасном для здоровья виде, и молодым людям они кажутся не такими уж и плохими и даже безобидными.

2. Социальные сети часто используют мошенники, и из-за недостатка определенного опыта и знаний их жертвами как раз часто и становятся студенты.

3. Всем известно, как затягивают социальные сети, и из-за этого у студентов может падать успеваемость. Порой, вместо того, чтобы готовиться к

зачету, студенты «провисают» в соцсетях и напросто убивают свое время, которое можно было потратить с пользой.

4. В социальных сетях трудно отфильтровать информацию и рекламу. Даже если студент интересуется только определенной тематикой, в соцсетях будет все равно вылезать другая информация, и из-за ее переизбытка человек больше утомляется и раздражается.

5. Иногда студенты заменяют реальное общение общением в соцсетях. Может доходить до того, что учащиеся становятся нелюдимыми и апатичными в реальной жизни, что отрицательно сказывается на их психологическом состоянии.

6. Иногда социальные сети угнетают некоторых учащихся, и они начинают чувствовать себя неполноценными. В соцсетях зачастую показывают идеальную картинку, которая совсем не похожа на реальность. Однако некоторые молодые люди ей верят и начинают сравнивать себя с кем-то другим, более красивым, умным, успешным и т.д. От этого появляется уныние, депрессивное состояние и порой даже суицидальные мысли.

7. Необходимы меры не только на международном, государственном, муниципальном уровнях, но и на уровне образовательной организации.

1.3 Информационные угрозы личности в сетевой коммуникации (информационные опасности сетевых коммуникаций)

Информационные угрозы личности в сетевой коммуникации можно разделить на три группы:

1. Информационно-технические опасности. К ним относятся, например, хакерский взлом сети, распространение вирусного программного обеспечения, кража данных с помощью специальных программ²².

²² Высшее образование в немецкой и русской традициях: колл. моногр. [Текст] / М. В. Богуславский, Е. В. Неборский, В. В. Неборская [и др.]; под общ. ред. М. В. Богуславского. Ижевск: Ин-т компьютерных исследований, 2019. С.56.

2. Информационно-психологические опасности. К ним относятся троллинг, преследование, унижение, оскорбление, шантаж, манипулятивные воздействия, методы социальной инженерии.

3. Смешанные опасности. Представляют собой сочетание информационно-технических и информационно-психологических приёмов. К ним относятся спам, фишинг, письма счастья и прочее.

Некоторые виды информационных угроз:

- Вредоносные программы. Их цель — причинить ущерб компьютеру, серверу или компьютерной сети.

- Программы-вымогатели. Способны блокировать доступ к компьютеру. Чтобы снять блокировку, жертву обманом заставляют заплатить выкуп.

- Троянская программа. Инструмент для атаки, замаскированный под легитимную программу.

- DoS-атаки и DDoS-атаки. Используются для перегрузки сетевых серверов в попытке выключить веб-сайт или онлайн-сервис на несколько минут, часов или даже дней.

- Создание фейковых аккаунтов. Через них злоумышленники получают доступ к личным сведениям.

В современном мире идет наращивание информационных ресурсов, которые являются важнейшим условием для устройства самой жизни человека. Информационная глобализация в настоящее время является наиболее показательным интеграционным процессом. Он включает развитие коммуникаций, использование космического пространства для передачи информации, рост глобальных информационных сетей, компьютеризации многих процессов жизнедеятельности человечества²³.

Информация создается человечеством с момента его зарождения и в процессе его развития. Четыре информационных революции подарили

²³ Уорли Б. Интернет: реальные и мнимые угрозы[Текст] / Б. Уорли. - М.: КУДИЦ-Образ, 2021. - 320 с.

человечеству такие средства и методы накопления, хранения и передачи информации, как письменность, книгопечатание, телефон, телеграф, радио, телевидение, компьютер, коммуникационные технологии.

Библия Иоганна Гутенберга, напечатанная в 1456 г., приоткрыла дверь в культурное пространство, а спустя 500 персональная компьютерная вездесущность широко распахнула ворота в информационный век.

Опыт развития мировых открытых сетей, например, Интернета, позволяет говорить о начале новой эры в развитии средств и систем переработки информации. В таких сетях пользователь воспринимает сам себя и воспринимается другими как неотъемлемый компонент единого информационного сообщества. Именно это обстоятельство требует внимательного анализа новых угроз, порожденных сетевой информационной революцией, физическому, психическому и социальному здоровью людей.

Все более острой становится проблема защиты права личности, общества, государства на конфиденциальность определенных видов информации. Каждый человек, доверяющий информацию о себе государственному органу или фирме, вправе рассчитывать на то, что она не будет разглашена или использована ему во вред.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность²⁴.

Поскольку сейчас межсетевые коммуникации различных типов являются важной составляющей повседневной жизни миллиардов человек, то прежде чем переходить к вопросу об информационной безопасности личности необходимо определить, что же непосредственно угрожает личности. Вообще, в каждой

²⁴ Бояркина Л.А., Бояркин В.В. Социальные сети как угроза персональным данным [Текст] / Л.А.Бояркина, В.В. Бояркин / Информационные технологии в профессиональной деятельности и научной работе: сборник материалов Всероссийской научно-практической конференции с международным участием.- Йошкар-Ола: Мар-ГТУ: в 2 ч.- ч. 1.- 2021.- С. 30-33.

сфере - экономике, политике, культуре, общении, - с которой взаимодействует личность, находятся свои собственные угрозы, связанные с получением или не получением какой-либо информации. Их важность может варьироваться от сферы к сфере, но в сущности все угрозы остаются одними.

Итак, угрозы информационной безопасности личности:

1. Угроза конфиденциальности информации, оставляемой человеком в различных сетевых коммуникациях;
2. Угроза достоверности информации, получаемой пользователем;
3. Угроза полноте информации, получаемой пользователем;
4. Угроза актуальности информации, получаемой пользователем;
5. Угроза «информационного голода»;
6. Угроза избыточности информации;

Рассмотрим каждую из этих угроз подробнее.

Угроза конфиденциальности информации, оставляемой человеком при различных сетевых коммуникациях.

Работая в Интернете, каждый из нас обязательно оставляет хоть какую-нибудь информацию о себе - иногда по собственному желанию, а иногда и по необходимости. И не всегда мы задумываемся о том, что в Интернете, как в американских детективах, «любая наша информация может использоваться против нас».

Наиболее частыми персональными данными, которые пользователь оставляет в Интернете, являются:

1. Адреса электронной почты, которые остаются при подавляющем большинстве регистраций на Интернет-ресурсах.
2. Персональные данные платежных систем, как реальных, так и виртуальных. А в случае Интернет-покупок - и реальные почтовые адреса.
3. Данные резюме на рекрутинговых ресурсах.
4. Приватные данные общего характера - привычки, интересы, предпочтения, публикуемые на личных страницах, блогах, социальных сетях, открытых медиа-хостингах.

5. Сконвертированные данные из законно созданных государственными и коммерческими организациями баз данных.

Опасность заключается в том, что раз вешав информацию, человек уже перестает ее контролировать. И далеко не факт, что информация о гражданине не будет использована во вред ему же. Конечно, чисто теоретически такая опасность существовала с того момента, как данные о гражданах вообще начали собирать - но именно Интернет-технологии неимоверно упростили в этом плане работу злоумышленникам. Во-первых, появилась возможность собрать много информации о множестве людей в одном месте. Во-вторых, информацию стало намного легче заполучить - взломать российскую базу можно аж из Америки, а для выноса сведений о миллионе людей нужна крошечная, замаскированная под кулон «флэшка». В-третьих, ее стало легче продать - Интернет-торговля позволяет сделать это анонимно и весьма удаленно. В результате персональные данные миллионов людей находятся в опасности попадания к преступникам - это явление на Западе получило название *identity theft*, то есть «кража идентичности».

Примеры каждого из этих случаев достаточно хорошо известны.

Буквально в мае 2021 года состоялась крупная кража частных данных с сайта в vshtate.ru - банка резюме, находящегося в тесной связи с одной из крупнейших мировых социальных сетей vkontakte.ru, ведущей достаточно активную экспансию как на мировой рынок, так и в различные сферы жизнедеятельности человека, например, в Интернет-торговлю. Путем прямого парсинга информации, выложенной в открытый доступ, были захвачены данные о карьерах тысяч пользователей, теперь они могут быть выложены на тех ресурсах, которым пользователи не давали разрешение на хранение и публикацию информации. И эта проблема может стать повсеместной. Решения же пока не существует.

То же самое касается и частных данных блогов, социальных сетей и прочих современных ресурсов. Однако здесь проблема становится еще более серьезной, ибо на этих ресурсах, пусть даже в открытом лишь для узкого круга

лиц доступе, могут выкладываться фотографии и видеоролики, компрометирующие честь и достоинство размещающего, а так же и его друзей. Причем, эта информация выкладывается без согласия всех лиц, которые заинтересованы в её открытии или сокрытии, а добиться удаления. Решения проблемы пока не существует²⁵.

Угроза достоверности информации, получаемой пользователем

Приведем лишь один серьезный пример этой угрозы.

Задача рекламы - представить товар в лучшем свете, вызвать у потребителя желание его приобрести. А самый распространенный рекламный продукт в России сегодня - средства для похудения, препараты для лечения суставов, сердечные и глазные, препараты, разные «повышатели» мужской потенции, медицинские приборы, гарантирующие моментальное избавление от всех болячек и т. п. Все это можно заказать по телефону за немалые деньги.

Современная реклама - страшная сила. Заклинания типов в белых халатах, которые вкрадчивым голосом вещают нам с телеэкрана «Ассоциация стоматологов / терапевтов / гинекологов рекомендует...», часто имеют большее влияние, чем советы настоящих профессионалов. А продолжительность рекламы непроверенных лекарственных средств на «Радио России» - государственной радиокompании - составляет несколько десятков часов в неделю.

В результате, вместо того, чтобы идти к врачу, человек пытается заглушить головную боль таблеткой, которая, судя по рекламе, «сильнее боли», а потом, к несчастью, узнает, что у него опухоль головного мозга. В последнее время врачи отмечают резкий рост жертв самолечения. По неофициальной статистике в нашей стране ежегодно выдается до двух тысяч свидетельств о смерти, причиной которой стали медикаменты, продаваемые «по телефону», а сотни тысяч людей страдают от побочного действия таких препаратов. А ведь

²⁵ Неборский Е. В., Богуславский М. В. Стратегические тенденции развития системы высшего образования в Российской Федерации[Текст] / Е. В.Неборский, М. В. Богуславский // Гуманитарные исследования Центральной России. 2017. № 2. С. 7–20.

если внимательно вслушиваться в рекламу, то можно узнать много интересного. Например, что некое средство «не лекарство и не БАД, а гель», а другое «не содержит никаких химических элементов». Кроме того, в рекламе постоянно звучат весьма «оптимистичные» высказывания о том, что если Вам больше 35-40 лет, то у Вас уже должен быть целый букет заболеваний, а чтобы их предупредить, необходимо начинать принимать рекламируемые препараты как можно раньше, начиная лет так с 18-20. Причем реклама перенасыщена специфическими медицинскими терминами, перечислением симптомов болезней и ужасных последствий (проснулись утром, открыли глаза - и ничего не увидели, ослепли; встать с кровати не можете - сустав полностью разрушился и т. п.). И очень неприятное впечатление складывается, когда препараты рекламируют известные артисты.

Аналогичные воздействия не редкость -это засорение теле- и радиоэфиров различными рекламными акциями, навязывание различных товаров, спам на веб-сайтах и вторжение спамеров в приватные области мессенджеров, социальных сетей и электронной почты. Рекламные ролики, врываясь в контекст фильмов, передач, - напрочь разбивают их целостность. Знаменитая пирамида Мавроди, совершила грандиозное обдирало-во населения России, не благодаря самому Мавроди, а благодаря... Лёне Голубкову - виртуальному монстру порождённому ТУ

Угроза полноте информации, получаемой пользователем

Биржевые сводки, курсы валют и их эквивалентов, тенденции к их изменению, с одной стороны, важны для обывателя, а с другой стороны, вся та информация, которая влияет на означенные величины, крайне важна для биржевых брокеров, политиков, аналитиков. Они тоже могут не получать полной информации, более того они её не получают.

Так же интересными выглядят некоторые теории, относимые массами к конспирологическим: о мировом кризисе, о терроризме и т.п.

Информация является очень ценным товаром, потому существует государственные разведки, разведки крупных и не очень крупных

коммерческих компаний, политические технологии. Все они построены на утаивании какой-либо получаемой информации. В конечном итоге страдает множество человек²⁶.

Угроза актуальности информации, получаемой пользователем

В качестве примера для этой угрозы подойдет и пример, приведенный в предыдущей угрозе. Также классическим примером является шутка о метеорологическом прогнозе, который сбывается в 100 % случаев, только не в то время и не в том месте.

Если говорить серьезно, сейчас в мире существует тенденция замалчивания правды об экологических катастрофах. Это было характерно для Советского Союза (в 1986 году взрыв на Чернобыльской АЭС замалчивался несколько дней, в результате чего погибли тысячи, десятки тысяч человек, не эвакуированные и не получившие врачебной помощи), это же характерно и для катастрофы на нефтеразработках в Мексиканском заливе. Соккрытие актуального положения дел немало повлияло на очередные колебания на мировом рынке.

Угроза «информационного голода»

Поскольку информация сейчас является не только товаром на глобальном рынке, но и предметом массового потребления, а иногда и культа, то при неравномерном распределении возможностей доступа к информации, а так же при намеренном «подсовывании» информации сомнительного качества, появляется расслоение общества по уровню доступа к информации. Между прочим, подобная стратификация напрямую влияет на уровень культуры. Выставки, театральные постановки, компакт-диски исполнителей, не звучащих на центральных каналах, - все это недоступно, например, провинциальным пользователям. Массовая культура несет в себе именно проблему

²⁶ Голышко А. В., Сомов А. Ю. Проблемы эколого-технического развития сетей сотовой связи. Вестник связи[Текст] / А. В. Голышко А. Ю., Сомов. 2018. № 10. С.67.

информационного голода как движущую силу появления субкультур. А далеко не все субкультуры безобидны.

Из всего вышесказанного следует, что проблема достаточно обширна, причем, что характерно, несет в себе труднопреодолимую составляющую в виде свойства информации к свободному распространению.

Формирование информационного общества - комплексная проблема, включающая как политико-экономические, социально-культурные, правовые так и технологические аспекты. В последнее время активно развиваются технологии, направленные на психологическое воздействие, И в таких технологиях используют самые современные достижения науки и техники, в частности телекоммуникационные и компьютерные технологии. Причиной развития подобных технологий являются самые разнообразные потребности бизнесменов, политиков, педагогов, ученых. Данные технологии задействованы в таких общественно значимых феноменах и процессах как реклама товаров, политическая реклама, выборы, различные геополитические процессы, войны и т.п.

Поэтому необходимо защищать не только информацию от неправомерных действий личности, но и личность от негативного воздействия информации.

В качестве воздействия на личность могут выступать:

- целенаправленное информационное давление с целью изменения мировоззрения, политических взглядов и морально-психологического состояния людей;
- распространение недостоверной, искаженной, неполной информации;
- использование неадекватного восприятия людьми достоверной информации.

Все это является проявлением информационного насилия, которое выражается в навязывании населению информации определенной направленности. При этом неизбежно попирается безопасность как отдельной личности, так и общества в целом.

Кроме чудодейственных эликсиров, нередко оказывающихся обычным фиточаем с петрушкой, зверобоем и сушеной морковкой, средства массовой информации навязывают гражданам России выгодные им (и их реальным хозяевам) оценки, мнения, электоральное поведение, формы и методы вложения денег.

А разве не является информационным насилием прославление культа силы и гангстеризма, оплевывание национальных культурных ценностей России? А вестернизация телевидения и кинематографа? Это тоже насилие над душами, умами людей²⁷.

Информационное насилие - это также и избыточность информации. Ежедневно поступающая масса сведений, фактов, оценок, рекомендаций, которые нередко противоречат друг другу и которые человеческое сознание не успевает как следует переварить, сбивает человека с толку и не даёт возможности самоопределиться - ни в интеллектуальном, познавательном, ни в нравственном отношении.

Рассмотренные выше проблемы присущи не только России, и в рамках одной страны решить их невозможно.

Информационная безопасность предполагает и означает состояние, когда в обществе созданы условия, обеспечивающие свободное развитие личности, семьи, государства, которые дают возможность объективно оценивать исторический процесс, истинную обстановку в мире, стране, регионе, вырабатывать и принимать самостоятельные решения на основе современной, достоверной информации, практического осознания и научного мировоззрения всего спектра гуманитарного знания, составляющего и создающего истинную духовность каждого народа.

²⁷ Долганина В. В., Кольцова И. В., Погребная О. В. Исследование интернет-зависимости у студентов педагогического вуза и меры профилактики [Текст] / В. В. Долганина, И. В. Кольцова, О. В. Погребная // Общество и личность: проблемы гуманизации современного социокультурного пространства: материалы VII Всерос. науч.-практ. конф.: сб. науч. ст. преподавателей, науч.-практ. работников, обучающихся вузов / отв. ред. С. Е. Шиянов, А. П. Федоровский. Ставрополь: АНО ВО СКСИ, 2019. С. 432–437.

Необходимо внести поправки в статью 24 Закона «О рекламе», чтобы реклама лекарств, медицинской техники, изделий медицинского назначения была разрешена только в местах проведения медицинских и фармацевтических выставок, семинаров, конференций и в предназначенных для медицинских и фармацевтических работников специализированных печатных изданиях.

Надо начинать переговоры о международно-правовой защите сетевых информационных ресурсов, в том числе данных персонального характера, интеллектуальной собственности, а также авторских прав на материалы, распространяемые в Интернете и других открытых сетях²⁸.

Необходимы меры не только на международном, государственном, муниципальном уровнях, но и на уровне образовательной организации. рассмотреть возможности контроля и ограничения распространения по сети Интернет непристойной и оскорбляющей общественную нравственность информации, недобросовестной рекламы, мошеннических операций и других материалов, оказывающих негативное воздействие на физическое, психическое и социальное здоровье людей.

Этим самым будет внесен важный вклад в обеспечение безопасности личности в информационной сфере.

Выводы по первой главе

²⁸ Гаврилов А. А., Нестеров Е. К., Оленьев В. В., Сомов А. Ю. Добровольный и вынужденный экологический риск при воздействии электромагнитного излучения, создаваемого системами сотовой связи [Текст] / А. А. Гаврилов, Е. К. Нестеров, В. В. Оленьев, А. Ю. Сомов. Известия Академии промышленной экологии. 2021. № 2. С. 45.

Информационная безопасность личности — это состояние защищённости жизненно важных интересов человека в информационной сфере от внутренних и внешних угроз. Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещённой законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Отрицательное влияние социальных сетей на студентов

Несмотря на все плюсы соцсетей, у них есть и свои недостатки:

1. Главная опасность социальных сетей для молодежи — это реклама и пропаганда наркотиков и алкоголя. Как правило, эти пагубные пристрастия подаются в соцсетях в привлекательном и безопасном для здоровья виде, и молодым людям они кажутся не такими уж и плохими и даже безобидными.

2. Социальные сети часто используют мошенники, и из-за недостатка определенного опыта и знаний их жертвами как раз часто и становятся студенты.

3. Всем известно, как затягивают социальные сети, и из-за этого у студентов может падать успеваемость. Порой, вместо того, чтобы готовиться к зачету, студенты «провисают» в соцсетях и напросто убивают свое время, которое можно было потратить с пользой.

4. В социальных сетях трудно отфильтровать информацию и рекламу. Даже если студент интересуется только определенной тематикой, в соцсетях будет все равно вылезать другая информация, и из-за ее переизбытка человек больше утомляется и раздражается.

5. Иногда студенты заменяют реальное общение общением в соцсетях. Может доходить до того, что учащиеся становятся нелюдимыми и апатичными в реальной жизни, что отрицательно сказывается на их психологическом состоянии.

6. Иногда социальные сети угнетают некоторых учащихся, и они начинают чувствовать себя неполноценными. В соцсетях зачастую показывают идеальную картинку, которая совсем не похожа на реальность. Однако некоторые молодые люди ей верят и начинают сравнивать себя с кем-то другим, более красивым, умным, успешным и т.д. От этого появляется уныние, депрессивное состояние и порой даже суицидальные мысли.

7. Необходимы меры не только на международном, государственном, муниципальном уровнях, но и на уровне образовательной организации.

ГЛАВА 2. МЕТОДИКА ФОРМИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ У СТУДЕНТОВ ПОО (НА БАЗЕ ОзТК)

2.1. Методы формирования информационной безопасности личности у студентов ПОО (на базе ОзТК)

Проблеме информационной безопасности в последнее время уделяется все больше внимания. Это связано с тенденцией постоянного роста информационных потоков в развивающемся информационном обществе, в котором информация становится средством достижения политических, экономических и технологических целей. Развивающиеся компьютерные технологии позволили увеличить информационный поток, сделав его ведущим социальным ресурсом, который вовлекает в себя все возрастные слои общества, ставя под угрозу секреты личности, общества и государства²⁹.

Некоторые методы формирования информационной безопасности личности у студентов учреждений среднего профессионального образования:

- Практические задания. Создание проектов с использованием программного обеспечения для обработки данных или представление информации в мультимедийной форме помогает развивать навыки работы с цифровыми инструментами.
- Занятия, на которых обсуждают основные угрозы и способы защиты. Студенты узнают о потенциальных угрозах, таких как вирусы, фишинг и утечки данных, и учатся применять практические меры по их предотвращению.
- Специальные мастер-классы или тренинги. Такие мероприятия могут включать практические задания, например анализ реальных случаев утечек данных или кибербуллинга. Это позволяет студентам не только понять теоретические основы, но и получить опыт практического применения полученных знаний.

²⁹ Нурпеисова Б. С., Давлетьярова М. А. Влияние социальных сетей на социализацию студенческой молодежи [Текст] / Б. С. Нурпеисова, М. А. Давлетьярова // Экономика и социум. 2017. № 8 (39). С. 196–200.

- Интеграция тем информационной безопасности в различные дисциплины. Например, в рамках учебного курса по основам экономики можно обсудить, как киберугрозы могут повлиять на бизнес-процессы, а в курсе по праву — рассмотреть вопросы защиты персональных данных.

- Использование активных методов обучения, в том числе с применением инструментов искусственного интеллекта. Например, для формирования пространственного представления о цифровой среде можно применить методические приёмы структурирования учебного материала, такие как интеллект-карта, кластеры и другие³⁰.

- Проведение бесед. Например, на темы «Безопасность при работе в сети Интернет», «Форумы и чаты в сети Интернет», «Сетевой этикет».

- Проведение мероприятий по профилактике киберпреступности. Для этого можно привлекать специалистов.

Ключевая идея в выборе и применении методов формирования информационной безопасности личности состоит в том, чтобы использовать техническую подготовку студентов как основу для проектной деятельности по информационной безопасности. Не просто рассказывать о правилах, а вовлекать их в создание продуктов и решений для безопасности.

Методы формирования информационной безопасности личности для ГБПОУ «Озерский технический колледж»

1. Проектно-практические методы (основанные на специфике технического колледжа)

«Лаборатория кибербезопасности» (Студенческий проект)

Суть: Создать на базе IT-специальностей студенческое объединение, которое занимается анализом угроз в соцсетях. Студенты могут исследовать фишинговые письма анализировать методы социальной инженерии в

³⁰ Саенко Л. А., Егоров М. В. Интернет-пространство как фактор формирования сетевого сообщества[Текст] / Л. А. Саенко, М. В. Егоров // Историческая и социально-образовательная мысль. 2015. Т. 7, № 1. С. 159–162.

популярных среди молодежи сообществах и готовить ежеквартальные отчеты-предупреждения для всего колледжа.

Такой проект использует профильные компетенции студентов (программистов, сетевиков), дает им реальный практический опыт и создает внутренний экспертный центр.

«Технический аудит личного профиля»

В рамках занятий по информатике или дисциплинам специализации студенты проводят аудит своих (или условных) профилей в соцсетях: проверяют настройки конфиденциальности, используют методы OSINT (открытой разведки) для поиска информации о себе, анализируют цифровой след.

Технически подкованные студенты лучше воспримут такой инструментальный подход. Это превращает скучные правила в интересную техническую задачу.

Кейс-чемпионаты по расследованию инцидентов.

Командам дается смоделированный инцидент утечки данных из соцсетей или взлома аккаунта. Студенты должны разработать план действий: технический (смена паролей, проверка на вирусы), коммуникационный (что сообщить друзьям?), правовой (куда обращаться?).

Кейсы развивают системное мышление, навыки работы в команде и действия в нестандартных ситуациях, что критически важно для технических специалистов.

2. Игровые и интерактивные методы

Деловая игра «Суд над соцсетью»

Студенты распределяют роли: «обвинение» (приводит аргументы о вреде соцсетей для приватности), «защита» (аргументы о пользе), «свидетели» (те, кто пострадал от утечки данных), «эксперты» (аналитики по ИБ). Игра заставляет глубоко погрузиться в проблему.

Студенты активно вовлекаются в процесс, развивают критическое мышление и ораторские навыки.

Квиз/Квест «Digital Sherlock»

Интерактивная игра по станциям в помещениях колледжа или в онлайн-формате. Задания: расшифровать сообщение с помощью шифра Цезаря, определить фишинговую ссылку, правильно настроить приватность в соцсети, ответить на вопросы о кибербуллинге.

Такой формат соответствует духу соревновательности, может быть организовано силами студсовета или волонтеров.

4. Обучающе-просветительские методы

«Инфо-спринты» на неделе адаптации первокурсников

Короткие (15-20 минут), динамичные и обязательные вводные занятия по ИБ для новичков. Акцент на самых частых рисках: «Как отличить фейкового друга?», «Какие фото нельзя выкладывать?», «Что делать, если аккаунт взломали?».

Это превентивная мера, которая сразу задает тон ответственного поведения в сети.

Веб-проект «Киберликбез от студентов ОзТК»

Силами студентов (возможно, в рамках учебных проектов или кружка) создать на сайте колледжа или в его официальной группе VK раздел/канал с памятками, инфографикой, разбором кейсов. Контент должен быть в молодежном стиле (мемы, короткие видео).

Веб-ресурс позволяет студентам самим генерировать контент на языке сверстников, что повышает доверие. Развивает их медиаграмотность.

4. Организационно-педагогические методы

Интеграция модуля по ИБ в соцсетях в учебные программы.

Включить темы по цифровой гигиене и безопасности в соцсетях в курсы «Информатики», «Основ безопасности жизнедеятельности (ОБЖ)», «Права» и профильные IT-дисциплины.

Пример для ОБЖ: Не только пожарная безопасность, но и информационная. На праве — разбор законодательства о клевете и нарушении приватности. Междисциплинарная интеграция создает систему непрерывного обучения, а не разовых акций.

Создание «Кибердружины» (волонтерский отряд)

Подготовить группу студентов-волонтеров, которые консультируют однокурсников по вопросам проблем в соцсетях (буллинг, мошенничество), выступают как первичные помощники и направляют к кураторам или психологу в сложных случаях.

Волонтерское движение в области кибербезопасности формирует среду поддержки и разгружает педагогов.

Кроме того, в период педагогической практики при собеседовании с администрацией колледжа нами были намечены следующие направления:

1. Старт с диагностики: Проведение анонимного анкетирования, чтобы выявить, с какими именно рисками уже сталкивались студенты.

2. Привлечение студсовета в качестве союзника и проводника идей. Они лучше знают, какой формат будет работать.

3. Использование сайта и соцсети колледжа. Официальные ресурсы — главный канал для распространения полезного контента, созданного студентами.

4. Партнерство с IT-компаниями: Приглашение специалистов по кибербезопасности из местных или федеральных компаний для проведения мастер-классов (в онлайн или офлайн формате). Это профориентационный бонус.

Такой комплекс методов превращает формирование информационной безопасности из скучного инструктажа в живую, практически значимую и соответствующую духу технического колледжа деятельность.

2.2. Опытно – практическая работа по формированию информационной безопасности личности у студентов ПОО (на базе ОзТК). Анализ опытно – практической работы.

Интернет-зависимость – это уже давно признанное психологическое заболевание, а зависимость от социальных сетей - её новая форма. Причины этого явления вполне объяснимы: у каждого человека есть явные и скрытые

потребности, которые он стремится удовлетворить, это может быть потребность в общении, самореализации, экономии времени или еще чего-то, а социальная сеть дает ощущение удовлетворения этих потребностей. И все это кажется очень доступным, стоит написать красивую цитату и тебе отвечают 10 человек; стоит загрузить новое фото и тебе скажут 10 человек, какой ты красивый; стоит сделать пару кликов и в друзьях уже новый интересный знакомый... Однако по сути это уход от реальности, подмена реального на виртуальное, которое только дает ощущение удовлетворения потребностей, а на самом деле Интернет не может заменить реальной жизни, и поэтому человеку хочется еще и еще, и еще, но чем больше он получает «общения» через Интернет, тем больше его хочется, а потребности все также остаются неудовлетворенными, по крайней мере, большинство из них³¹.

Подобная зависимость постепенно развивается у многих людей, которые единожды попали в социальную сеть. Человек «подсаживается на сеть», и чем больше времени он ею пользуется, тем сложнее ему жить реальной жизнью. Почувствовать это сложно, нужно на несколько дней оторваться от компьютера, и только тогда возникнет целый букет чувств, начиная от сильного желания зайти в Интернет и заканчивая серьезной депрессией, это и есть симптомы зависимости. Зависимость приводит к множеству проблем: появляются комплексы, депрессия, страхи, перепады настроения и даже сексуальные расстройства.

Это психологическое заболевание и, как любая болезнь, требует лечения. Лечить любые психологические проблемы сложно, а тем более зависимости. Прежде всего, нужно осознать наличие проблемы и признать её для самого себя. Вторым шагом лечения должно стать замена виртуального общения на реальное, и постепенно с помощью друзей и родственником можно будет вылечиться.

³¹ Ковалевская Е. В. Общение студентов в социальных сетях [Текст] / Е. В. Ковалевская // Социолог 2.0: трансформация профессии: материалы VIII междунар. социол. Грушинской конф. / отв. ред. А. В. Кулешова. М., 2018. С. 409–412.

1. Анкетирование студентов ПОО (на базе ГБПОУ ОзТК)
1. Есть ли у тебя компьютер? а) да; б) нет
2. Есть ли подключение к сети? С помощью чего?
 - а) проводное б)- wi-fi в) - модем
1. В какой социальной сети зарегистрирован?
 - а) Face Book б) ВК в) Твитер г) одноклассники д) другая – какая?
1. В какое время ты заходишь на свою страничку?
 - А) когда есть время
 - Б) во время учебы
 - В) нахожусь там весь день
 - Г) только вечером после уроков
 - Д) ночью
1. Сколько времени в сутки уделяешь социальным сетям?
 - А) 20% Б) 50% В) 80%
1. Твои родители зарегистрированы в социальных сетях? а) да; б) нет
2. Где носишь телефон?
 - А) в кармане
 - Б) в сумке, в рюкзаке
1. Предпочитаешь живую беседу или же диалог в социальных сетях?
 - А) живую беседу Б) соц.сети в) смотря с кем
1. Как относишься к тому, что из-за социальных сетей люди стали необщительными, замкнутыми?
 - А) положительно Б) отрицательно в) все равно
1. Сколько времени можешь обойтись без социальной сети?
 - А) день Б) пять дней В) неделю г) невозможно
1. Любишь читать художественную литературу? А) да Б) нет
1. Посещаешь ли, центры культуры? (музеи, театры, выставки)
 - А) посещаю Б) не люблю данные мероприятия
1. Считаешь ли ты, что социальные сети, являются в какой- то мере “ вредом, поработившим человечество”?

А) да, люди стали раздражительней и зависимы от социальных сетей

Б) нет, не вижу никакого вреда

1. Общаясь в соц.сетях ты пишешь : *(выбрать несколько вариантов)*

А) Грамотно

Б) Вежливо

В) не обращая внимания на грамотность

Г) используя ненормативную лексику

Д) сокращая слова (спасибо- сп, спс)

Е) смотря, с кем общаюсь

1. Переносишь ли ты общение в соц. сетях на живое общение?

А) да так удобней и легче Б) нет, не переношу.

1. Взламывали ли твою страницу? А) да Б) нет

1. Социальные сети и вирусы не совместимы и не оказывают влияния друг на друга - так ли это? А) да Б) нет

1. Как относишься к тому, что информация вашей страницы доступна всем?

А) мою информацию видят только друзья

Б) мне все равно - пусть видят

В) положительно, я ищу новые знакомства

Г) я этого не знал

Д) свой вариант

1. Как вы думаете, какое значение имеет соц. сеть в обществе?

(выбрать несколько вариантов)

А) положительное - она сближает людей на расстоянии

Б) Отрицательное, она делает людей замкнутыми необщительными

В) помогает находить нужную информацию о людях

Г) Она дешевле и помогает решить многие вопросы

Д) Помогает объединить людей по интересам (положительным и отрицательным)

Е) Бесконтрольное общение

Ж) Не имеет временных ограничений

З) разрешен доступ к разной информации без возрастных ограничений

Результаты исследования

- Большинство подростков ГБПОУ ОзТК создает, по крайней мере, основной профиль, с их именем, возрастом, статусом, фотографией и интересами, но многие идут намного далее. Много подростков наносят регулярные визиты, чтобы обновить их профили и посетить профили других;

- 87 % студентов ГБПОУ ОзТК зарегистрированы более, чем в трех социальных сетях;

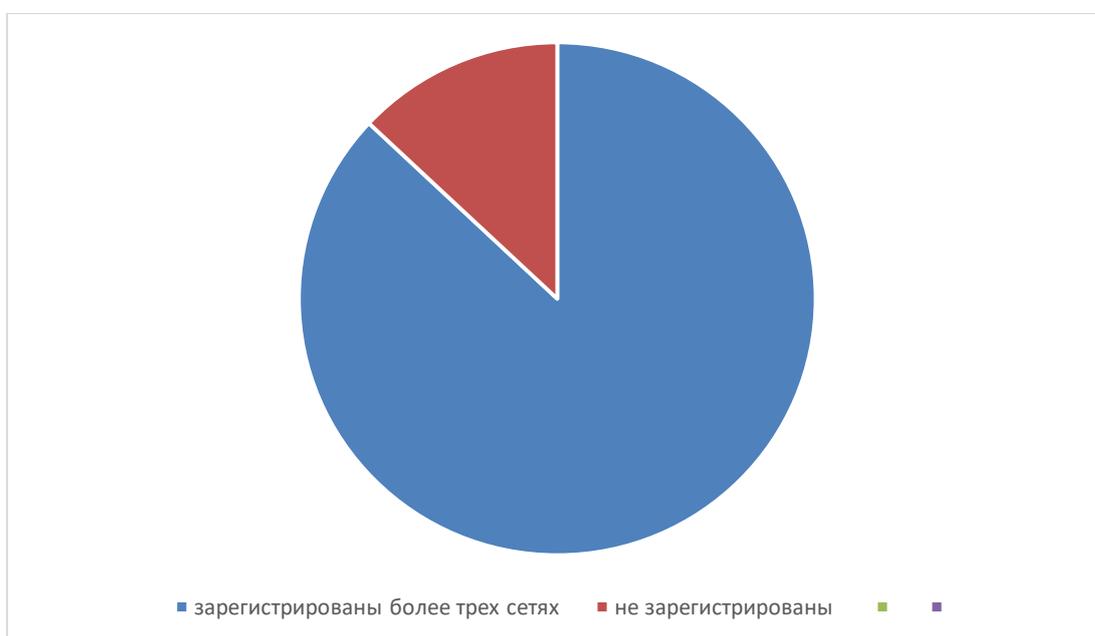


Диаграмма 1 - Результаты исследования

- 30% подростков ГБПОУ ОзТК признались, что их родители тоже имеют свои странички и постоянно там «висят»;

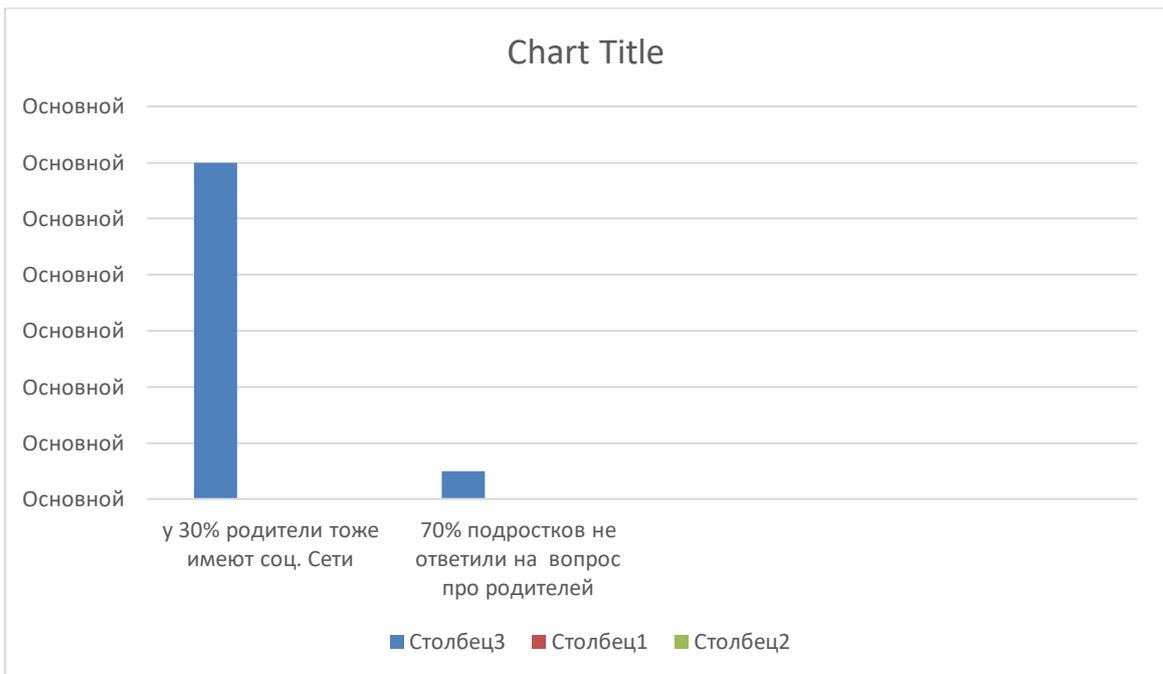


Диаграмма 2 - Результаты исследования.

- общение - ключевой аспект использования социальных сетей для студентов ГБПОУ ОзТК. А также подростки могут повесить общественные объявления. Большинство подростков использует сайты, чтобы поддержать отношения с их текущими друзьями;
- приблизительно 60 % подростков также используют сайты, чтобы завести новых друзей;

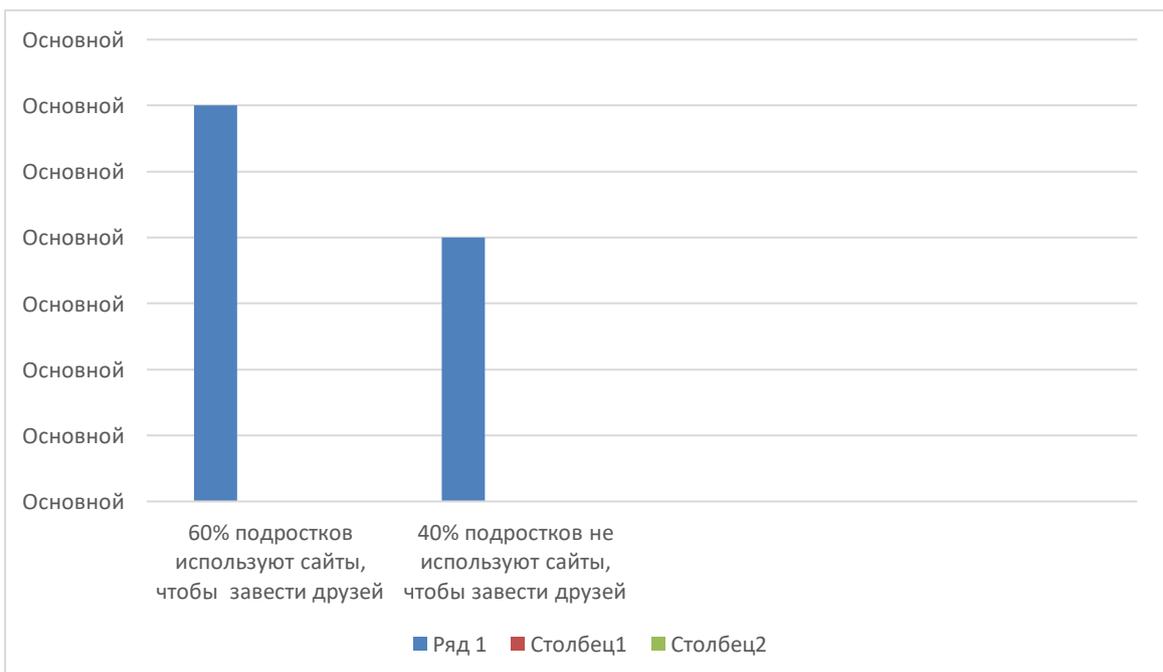


Диаграмма 3 - Результаты исследования.

- 73,8 % подростков ГБПОУ ОзТК не обращают внимание на грамотность и культуру общения, и не считают это необходимым для общения сверстников;

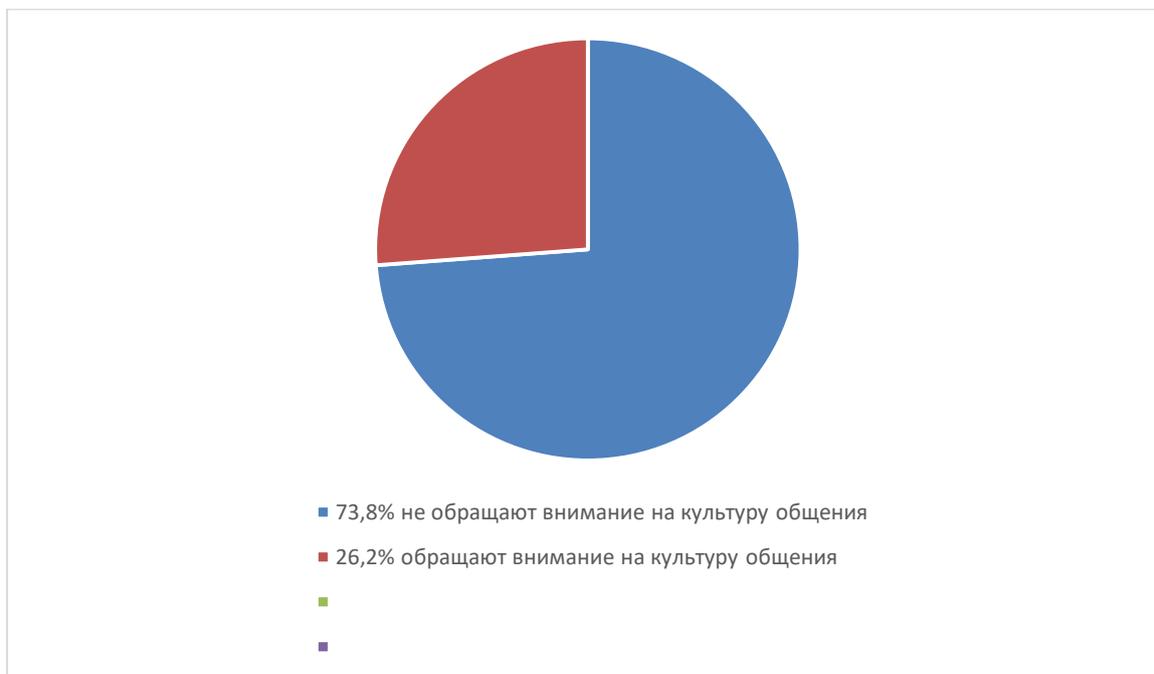


Диаграмма 4 - Результаты исследования.

- 35, 7% подростков ГБПОУ ОзТК используют сайты, чтобы сделать социальные планы с их друзьями, и иногда флиртовать;

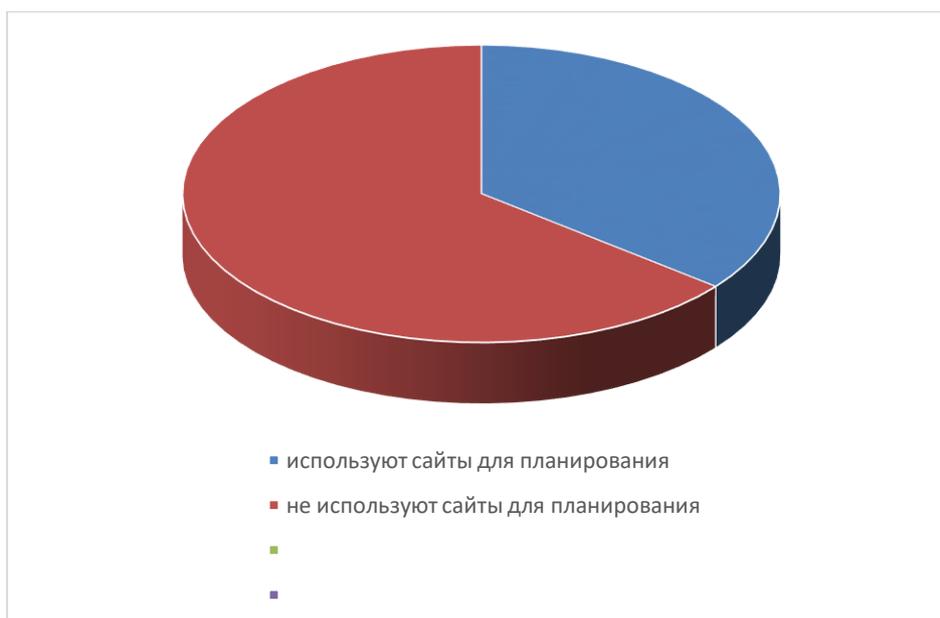


Диаграмма 5 - Результаты исследования.

- 42 % проверяют свои аккаунты в социальных сетях более 5 раз в день;

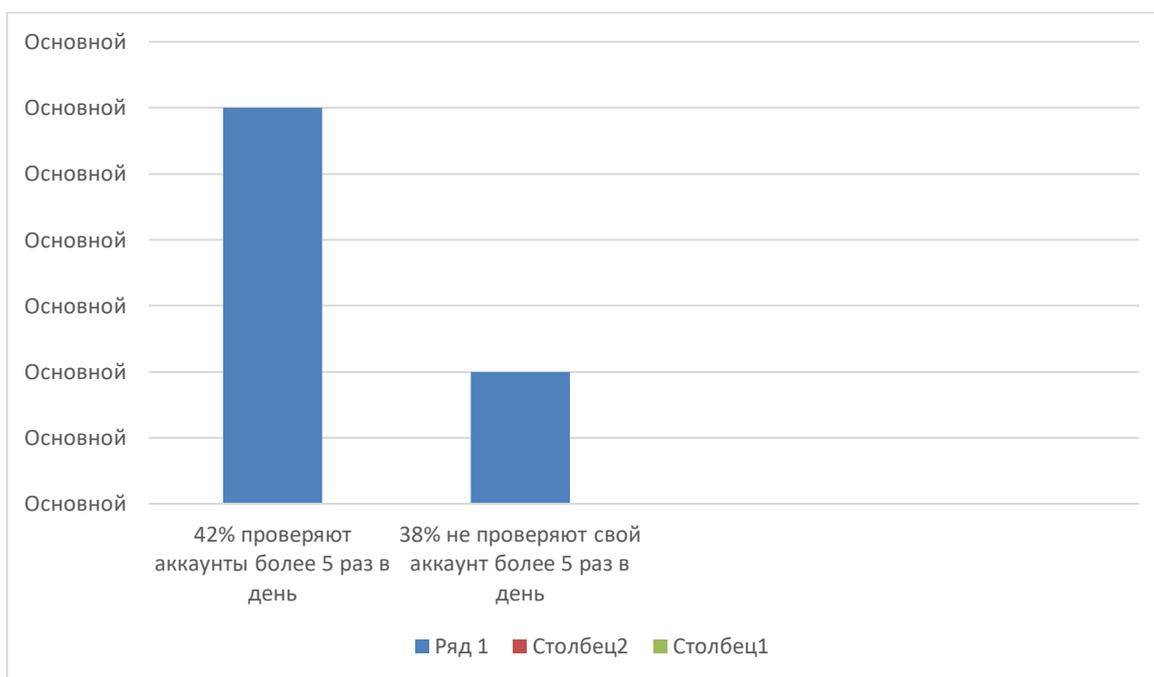


Диаграмма 6 - Результаты исследования.

- 14 % создают фальшивые аккаунты, не удостоверяющие их личность;

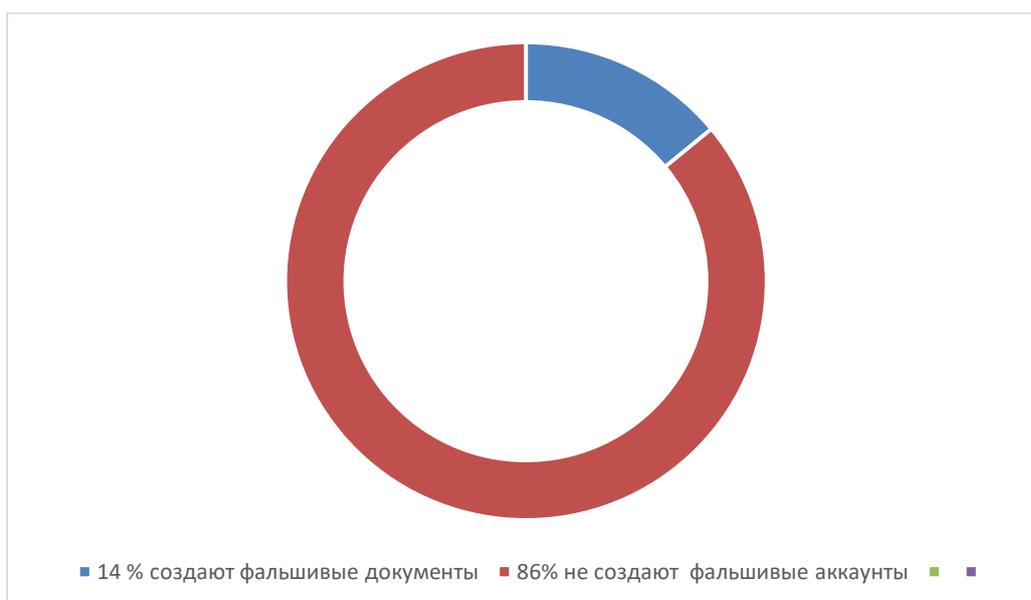


Диаграмма 7 - Результаты исследования

- 83% студентов ГБПОУ ОзТК занимаются хакерством, в основном для развлечения;

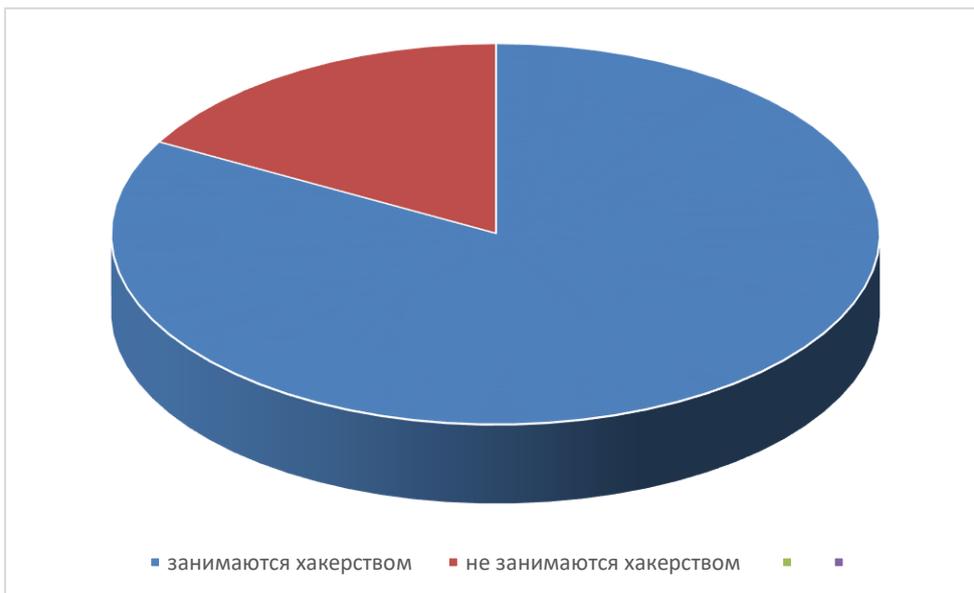


Диаграмма 8 - Результаты исследования.

- 91% студентов ГБПОУ ОзТК находятся в социальных сетях постоянно;

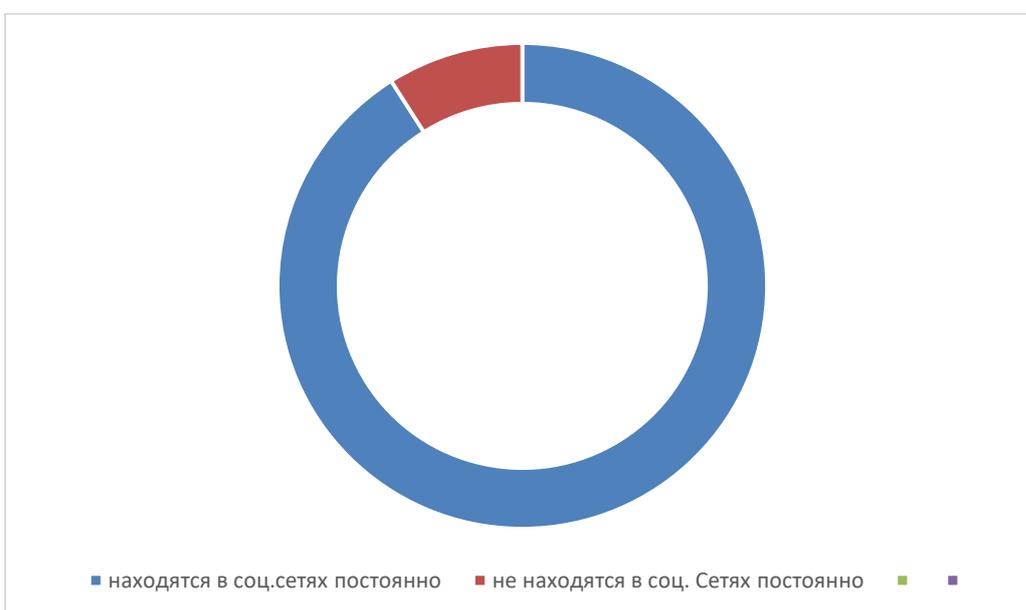


Диаграмма 9 - Результаты исследования.

- только 7% студентов ГБПОУ ОзТК видят в социальных сетях опасность.

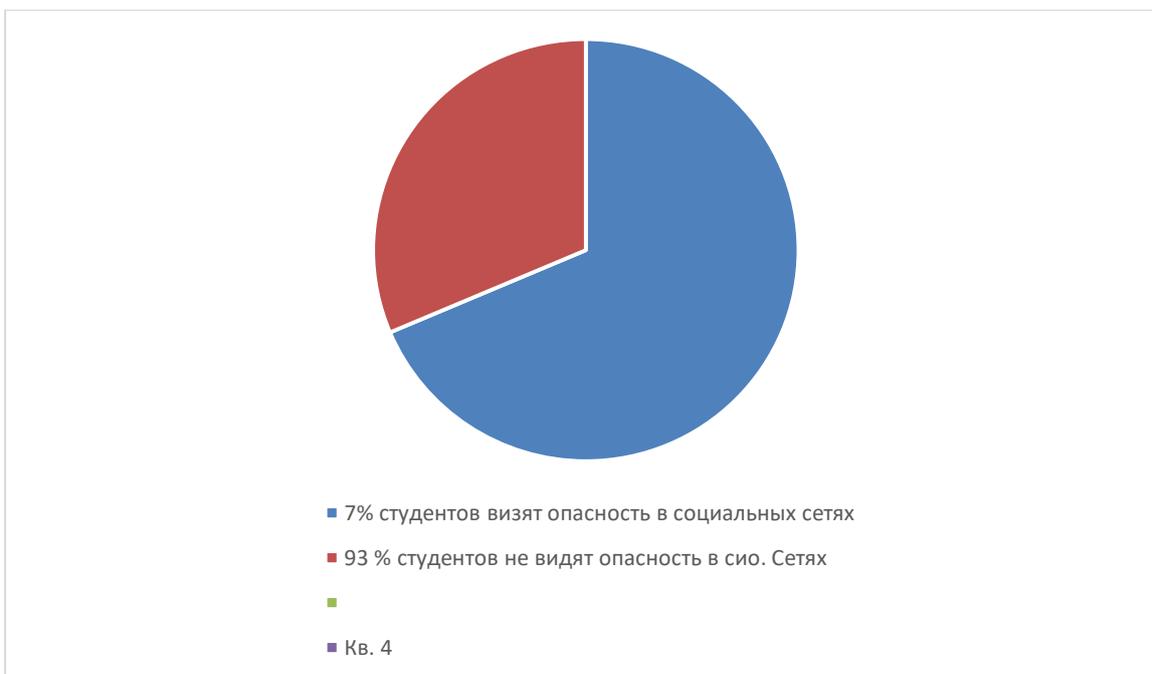


Диаграмма 10 - Результаты исследования.

Вывод: Опрос показал средний уровень компетентности учащихся в вопросах, связанных с информационной безопасностью в сети интернет. Большая часть студентов, недостаточно владеет информацией о видах угроз в сети Интернет и методах борьбы с ними.

Большинство придерживаются основных мер защиты, таких как ограничение раскрытия контактов и личной информации. Однако существуют различия в предпочтениях и восприятии эффективности возможных мер безопасности.

2.3. Разработка рекомендаций

Таким образом, я: 1. Провела беседы со студентами, 2. Продиагностировала — см. п.2.2., проанализировала, 4. провела квест, 5. обобщила результаты, 6. поработала с сайтом — обобщила результаты.

Некоторые трудности, с которыми я столкнулась:

- Излишне оптимистичная оценка уровня своей защищённости. Это может быть следствием недооценки угроз либо недостаточного уровня медийно-информационной грамотности.

- Различия в предпочтениях и восприятии эффективности возможных мер безопасности. Например, некоторые студенты считают, что к эффективным способам защиты аккаунта и личности относятся отсутствие контактов на личной странице, своевременный выход из аккаунтов на чужих.

- Трудности с анализом психологических угроз в социальных сетях, например, диалогов злоумышленника и жертвы. Это связано с отсутствием чётких критериев для оценки сообщений как противоправных и деструктивных, так как зачастую используются тонкие манипулятивные приёмы.

Рекомендации студентам по использованию социальных сетей

1. Положительные черты влияния социальных сетей:

- Возможность самореализоваться в глазах друзей и знакомых.
- Найти себе друзей, знакомых одноклассников
- Поиск в соц. сетях единомышленников. Есть немало важных и нужных групп, где люди могут обмениваться накопленным опытом или просто своими взглядами на жизнь.

- Большая база данных видео файлов, музыкальных файлов, среди которых можно найти редкие или нужные экземпляры.

2. Отрицательные черты влияния социальных сетей.

– Стесненная поза, сидячее положение в течение длительного времени.

Сидя за компьютером, студент (или взрослый) вынужден принять определенное положение, и не изменять его до конца работы.

– Воздействие электромагнитного излучения.

Современные мониторы стали безопаснее для здоровья, но еще не полностью. Вокруг монитора существуют электростатические и электромагнитные поля.

– Утомление глаз, нагрузка на зрение.

Именно из-за нагрузки на зрение через непродолжительное время у студентов возникает головная боль и головокружение. Если работать на компьютере (мобильном телефоне) достаточно долго, то зрительное переутомление может привести к устойчивому снижению остроты зрения.

– Перегрузка суставов кистей.

Постоянная перегрузка суставов и кистей может привести к повреждению суставного и связочного аппарата кисти, а в дальнейшем заболевания кисти могут стать хроническими.

– Стресс при потере информации.

Если компьютер "зависает" теряется важная и полезная информация, замедляется работа компьютера, то это может вызвать нервозность, повышение давления, ухудшение сна.

-Зависимость от виртуального мира.

Это самая распространенная проблема.

- Общедоступность информации.

Пользователи с легкостью добавляют информацию о себе, чем и могут воспользоваться заинтересованные в этом люди.

– Психические расстройства.

При проблемах в реальной жизни, общении с другими людьми человек ищет то, что ему не хватает в книгах, просмотрах TV, компьютере. Поэтому порой он погружается в компьютерный мир полностью, забывая про реальный мир.

Выводы по второй главе

Таким образом, можно выделить пути решения проблем, связанных с использованием социальных сетей студентами:

- Необходимо создать условия для осознанного взаимодействия в социальных сетях
- Необходимо создать условия для оказания большего внимания своей реальной жизни (проблемам в школе, в семье, друзьям);
- Необходимо создать условия для увеличения времени пребывания в компании друзей;

- Необходимо создать условия поиска альтернативных способов времяпрепровождения (например, занятия спортом, рисование, вышивание, чтение книг и т.п.).

Нельзя однозначно судить о влиянии социальных сетей на личность подростка. Конечно же, во всем есть свои минусы и плюсы. Следует лишь помнить, что все нужно делать с чувством меры, в том числе и пользоваться Интернетом.

ЗАКЛЮЧЕНИЕ

Таким образом, в работе проанализированы теоретические подходы к проблеме информационной безопасности личности в социальных сетях в психолого-педагогической литературе, выявлено понятие «информационная безопасность личности в социальных сетях», определены имеющиеся угрозы, уязвимости и направления для их минимизации.

Проведена диагностика текущего уровня информационной безопасности и выявлены типичные модели рискованного поведения студентов ПОО в социальных сетях (на базе ОзТК)

Определены педагогические условия и ресурсы образовательной организации для формирования информационной безопасности студентов.

Таким образом, во все времена информация играла чрезвычайно важную роль, которая из года в год становилась всё существеннее. В современном обществе она является одним из ключевых экономических ресурсов. Всем

хорошо известно, что «кто владеет информацией, тот владеет миром». Действительно, владение ей в достаточном количестве помогает человеку правильно оценить происходящие вокруг него события, разработать варианты своих действий и принять обдуманное решение. Поскольку информация представляет собой ценность, она может стать объектом купли-продажи, даже кражи (несанкционированного доступа), поэтому она и поддерживающая её инфраструктура должны быть защищены. Кроме того, информация - сильнейшее средство воздействия на личность, общество и мир в целом. Именно поэтому человечеству в современных условиях требуется механизм фильтрации информации, а впоследствии также инструмент защиты от нежелательной и (или) негативной информации.

Мир стремительно меняется, и, переходя в стадию информационного общества, изменяет все стороны жизни современного человека, независимо от того ребенок это или взрослый. Практически ежесекундно человек подвергается воздействию разнообразной информации, характер которой меняется от полезного и необходимого до откровенно агрессивного, манипулятивного. Каждая единица информации, каждое слово, знак, текст несет смысловую нагрузку, воздействующую на ценности человека, его привычки, мотивацию. Устное или печатное слово влияет на психику, зачастую подавляя личность, манипулируя ею. Переход общества на новый информационный уровень развития обуславливает актуализацию проблемы информационной безопасности. Исходя из всего вышеизложенного, возникает проблема информационной безопасности, и прежде всего именно личности как носителя индивидуальных способностей, характера, интересов. Вообще, проблема информационной безопасности чрезвычайно многогранна.

В ней можно выделить несколько важных аспектов. Во-первых, собственно информационный аспект, связанный с защитой непосредственно информации и информационных ресурсов. К сожалению, большинство существующих нормативных документов рассматривают информационную безопасность именно в этом контексте, оставляя за гранью, проблемы личности.

Информационная безопасность личности - это: а) состояние защищённости, при котором отсутствует угроза причинения вреда информации, которой владеет личность; б) состояние и условие жизнедеятельности личности, при которых отсутствует угроза нанесения вреда личности информацией. И отсюда следует разделить информационную безопасность на информационно-идеологическую и информационно-техническую.

При этом под информационно-технической безопасностью личности следует понимать защищенность информации от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба личности, а под информационно-идеологической безопасностью - защищенность личности от преднамеренного или непреднамеренного информационного воздействия, имеющего результатом нарушение прав и свобод в области создания, потребления и распространения информации, пользования информационной инфраструктурой и ресурсами, противоречащего нравственным и этическим нормам, оказывающих деструктивное воздействие на личность, имеющих негласный (внечувственный, неосознанный) характер, внедряющих в общественное сознание антисоциальные установки.

Информационная безопасность личности - это состояние и условие жизни личности, при которой реализуются ее права и свободы. Жизненно важные интересы - совокупность потребностей, удовлетворение которых обеспечивает существование и возможности прогрессивного развития личности, общества и государства. К жизненно важным интересам личности относятся: соблюдение и реализацию конституционных прав на поиск, получение, производство и распространение информации; связанные с реализацией права граждан на неприкосновенность частной жизни; использование информации в целях духовного, физического, интеллектуального развития; защиту прав на объекты интеллектуальной собственности; обеспечение прав гражданина на защиту своего здоровья от неосознаваемой человеком вредной информации. Угроза

безопасности - совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

Угрозами информационной безопасности личности являются: принятие нормативных актов, противоречащих конституционным правам граждан; противодействие реализации гражданами прав на неприкосновенность частной жизни; неправомерное ограничение доступа к открытой информации; нарушение прав граждан в области массовой информации. противоправное применение специальных средств, воздействующих на сознание человека; манипулирование информацией. Источниками угроз информационной безопасности личности также могут выступать другая личность, программные и технические средства, группа лиц, общественная группа или даже государство, интернет, СМИ. Необходимо отметить, что в нашей стране отсутствует разработанная нормативная база, обеспечивающая информационную безопасность личности и государства. Практически, мы можем назвать лишь два документа: Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895), и Указ Президента РФ от 12 мая 2004 г. N 611, с дополнениями в 2004 и 2005 гг. «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена».

Таким образом, имеется проблема, связанная с разнообразным информационным воздействием на психику человека, и те негативные последствия, которые могут за этим воздействием последовать. В специальной литературе описаны случаи тяжелых форм зависимости связанные с взаимодействием человека глобальными информационными сетями, разнообразные формы игромании, правонарушения, связанные с воздействием информации на личность подростка.

Таким образом, складывается ситуация, когда ни органы власти, ни система образования, ни какие-либо другие социальные институты не в силах контролировать поток информации, обрушивающийся на человека. В этих

условиях, проблема информационной безопасности личности человека приобретает ярко выраженный социально-педагогический смысл.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ:

1. Бояркина Л.А., Бояркин В.В. Социальные сети как угроза персональным данным [Текст] / Л.А.Бояркина, В.В. Бояркин // Информационные технологии в профессиональной деятельности и научной работе: сборник материалов Всероссийской научно-практической конференции с международным участием.- Йошкар-Ола: Мар-ГТУ: в 2 ч.- ч. 1.- 2021.-352с.

2. Вараксин А. В. Влияние социальных сетей на формирование ценностных ориентиров современной молодежи [Текст] / А. В. Вараксин // Преподаватель XXI век. -2016. -№ 2. -С. 205–212.

3. Высшее образование в немецкой и русской традициях: колл. моногр. [Текст] / М. В. Богуславский, Е. В. Неборский, В. В. Неборская [и др.]; под общ.

ред. М. В. Богуславского. Ижевск: Ин-т компьютерных исследований, 2019. - 895с.

4. Гаврилов А. А., Нестеров Е. К., Оленьев В. В., Сомов А. Ю. [Текст] / А. А.Гаврилов, Е. К.Нестеров, В. В.Оленьев, А. Ю. Сомов Добровольный и вынужденный экологический риск при воздействии электромагнитного излучения, создаваемого системами сотовой связи. Известия Академии промышленной экологии. -2021. -№ 2. -С.45.

5. Галатенко В. А. Информационная безопасность В. А. [Текст] / Галатенко // Открытые системы. -2021. -№ 1 (15). -С. 38—43.

6. Гафарова Г. Г., Смелянская В. В. Информационная безопасность личности [Текст] / Г. Г.Гафарова, В. В. Смелянская // Безопасность личности: состояние и возможности обеспечения : материалы междунар. науч.-практ. конференции 10—11 мая 2012 года. Ереван, Пенза, Колин : Социосфера, 2019.- 854с.

7. Гольшко А. В., Сомов А. Ю. Проблемы эколого-технического развития сетей сотовой связи. Вестник связи [Текст] / А. В.Гольшко, А. Ю.Сомов. -2018. -№ 10. -С.67.

8. Григорьев Ю. Г. Сотовая связь: радиобиологические проблемы и оценка опасности. Радиационная биология. Радиоэкология [Текст] / Ю. Г.Григорьев. - 2019. -№ 5.- С.56.

9. Григорьев Ю. Г. Эмоциональный стресс и электромагнитные поля. Ежегодник Российского Национального Комитета по защите от неионизирующих излучений [Текст] / Ю. Г.Григорьев . М.: Изд-во РУДН, 2021. -854с.

10. Долганина В. В., Кольцова И. В., Погребная О. В. Исследование интернет-зависимости у студентов педагогического вуза и меры профилактики [Текст] / В. В. Долганина, И. В.Кольцова, О. В.Погребная // Общество и личность: проблемы гуманизации современного социокультурного пространства: материалы VII Всерос. науч.-практ. конф.: сб. науч. ст.

преподавателей, науч.- практ. работников, обучающихся вузов / отв. ред. С. Е. Шиянов, А. П. Федоровский. Ставрополь: АНО ВО СКСИ, 2019. -895с.

11. Еркин А. В. Понятия «информация» и «информационная безопасность»: от индустриального общества к информационному [Текст] / А. В. Еркин // Информационное общество. -2020. -№ 1. -С. 73.

12. Закупень Т. В. Понятие и сущность информационной безопасности и ее место в системе обеспечения национальной безопасности РФ [Текст] / Т. В. Закупень // Информационные ресурсы России. -2021. -№ 4. -С. 28—34.

13. Зейналов З. З. Проблемы определения информации как объекта информационных правоотношений [Текст] / З. З. Зейналов // Информационное право. -2019.- № 1. -С. 10.

14. Иванов С. В. Правовое регулирование информационной безопасности личности в Российской Федерации [Текст] / С. В. Иванов // Вестник Екатеринбургского института. -№ 1 (25). -2019.- С. 50.

15. Кагель Г. Информационная эпоха: экономика, общество и культура [Текст] / Г.Кагель. М. : ГУ ВШЭ, 2018. -754с.

16. Ковалева Н. Н. Информационное право России [Текст] / Н. Н.Ковалева: учеб. пособие. М. : Дашков и Ко, 2017. -369с.

17. Ковалевская Е. В. Общение студентов в социальных сетях [Текст] / Е. В. Ковалевская // Социолог 2.0: трансформация профессии: материалы VIII междунар. социол. Грушинской конф. / отв. ред. А. В. Кулешова. М., 2018. -452с.

18. Кузьмин В. П. Понятие и юридическая сущность информации и пути формирования информационного общества в России [Текст] / В. П. Кузьмин // Информационное право. -2019. -№ 2. -С. 3.

19. Малюк А. А. Информационная безопасность [Текст] / А. А. Малюк концептуальные и методологические основы защиты информации : учеб. пособие для вузов. М. : Горячая линия — Телеком, 2018. -412с.

20. Неборский Е. В., Богуславский М. В. Стратегические тенденции развития системы высшего образования в Российской Федерации [Текст] / Е.

В.Неборский, М. В. Богуславский // Гуманитарные исследования Центральной России. -2017. -№ 2. -С. 7–20.

21. Нурпеисова Б. С., Давлетьярова М. А. Влияние социальных сетей на социализацию студенческой молодежи [Текст] / Б. С.Нурпеисова, М. А. Давлетьярова // Экономика и социум. -2017. -№ 8 (39). -С. 196–200.

22. Ожегов С. И. Словарь русского языка : Около 57 000 слов [Текст] / С. И. Ожегов / под ред. д-ра филол. наук, проф. Н. Ю. Шведовой. 14-е изд., стереотип. М. : Рус. яз., 1982. -741с.

23. Просвирнин В. Г., Просвирнин Ю. Г. Понятие и правовые основы информационных технологий [Текст] / В. Г.Просвирнин, Ю. Г. Просвирнин // Юридические записки. -2019. -№ 2 (25). -С. 151.

24. Реснянская М. А., Кузьмина С. В. Влияние социальных сетей на мировоззрение студентов [Текст] / М. А.Реснянская, С. В. Кузьмина // Молодой ученый. -2016. -№ 9.4. -С. 61–63.

25. Саенко Л. А., Егоров М. В. Интернет-пространство как фактор формирования сетевого сообщества [Текст] / Л. А.Саенко, М. В. Егоров // Историческая и социально-образовательная мысль.- 2015. Т. 7, -№ 1. -С. 159–162.

26. Саенко Л. А., Егоров М. В. Сетевое общество в контексте современных социальных трансформаций [Текст] / Л. А.Саенко, М. В. Егоров // Дискуссия.- 2018. -№ 7 (48). -С. 88–93.

27. Стрельцов А. А. Обеспечение информационной безопасности России. Теоретические и методологические основы [Текст] / под ред. В. А. Садовниченко и В. П. Шерстюка М. : МНЦМО, 2019. -563с.

28. Уорли Б. Интернет: реальные и мнимые угрозы [Текст] / Б.Уорли. - М.: КУДИЦ-Образ, 2021. -452с.

29. Хараш А. У. Психология одиночества [Текст] / А. У. Хараш // Педология. 2000. № 4 (ноябрь). С. 7–16. 14. Цой Н. А. Феномен интернет-зависимости и одиночества // Социологические исследования. -2019. -№ 12.- С. 98–107.

30. Чернов А. А. Становление глобального информационного общества[Текст] / А. А.Чернов проблемы и перспективы. М., 2020. -147с.

31. Шершнева Л. И. Информационная безопасность России [Текст] / Л. И. Шершнева // Безопасность. -2021. -№ 11—12. -С. 49—50.

Приложение 1

«Памятка поведения в социальных сетях для студентов»

Если Вы безответственны, то ваше поведение в социальных сетях может нанести вред как личной, так и профессиональной сфере. Это правило касается не только взрослых людей, но и подростков, устраивающихся на работу.

Итак, несколько простых правил:

1. Не хвастайтесь незаконной деятельностью.

Никаких роликов незаконной деятельности! Компромат может вылиться в административное или даже уголовное наказание. Раз-два в год просматривайте Ваш контент в соц.сетях, чтобы удалить все компрометирующие фото.

2. Не высказывайте агрессии.

Когда студент обращается к социальным сетям, блогам и форумам, чтобы поиздеваться над кем-нибудь, риски могут оказаться неизмеримыми. Этому студенту грозит не только отчисление, но серьезная уголовная статья.

3. Разглашение конфиденциальной информации.

Молодые люди особенно уязвимы перед лицом интернет-хищников и воров личных данных. Любые личные данные, опубликованные в соц.сетях, могут помочь ворам и коррупционерам нанести Вам вред. Даже фотография, на которую случайно попала ваш студенческий билет или ксерокс аттестата. То же самое касается и Вашего местонахождения. В частности, никогда не пишите в социальных сетях, что Вы находитесь дома один или куда-то уехали.

4. Нельзя лгать, жульничать и заниматься плагиатом.

Соврали, что нужно доделать курсовую, а сами отправились на концерт? Если при этом Вы поменяли статус в соц. сети и выложили кучу фотографий – время задуматься, не повлияет ли это на Вашу оценку.

5. Нельзя угрожать расправой.

Даже публикация анонимной, бессмысленной угрозы на сомнительном интернет-форуме, где полно посторонних людей, будет служить тревожным сигналом. И как только властям удастся локализовать угрозу, они имеют полное право начать расследование.

6. Нельзя публиковать свидетельства своего непрофессионализма.

Иногда даже информация сугубо личного характера, размещенная в профилях социальных сетей, может послужить тревожным знаком для потенциального работодателя. В современную эпоху прозрачности идеальным является профессиональный профиль.

7. Нельзя полностью полагаться на настройки конфиденциальности.

Как бы прилежно вы ни пытались защитить свои личные данные в социальных сетях, лучше всего привыкнуть к мысли о том, что вся опубликованная вами информация может стать известной вашим родителям, руководству и незнакомым людям. Полагайтесь на свое благоразумие.

8. Лучше не выкладывайте информацию в состоянии эмоционального возбуждения.

Публикация гневного твита в порыве бешенства может принести вам облегчение, однако минутное удовольствие, которое вы получите от его публикации, не стоит того потенциального вреда, который он может причинить. Остановитесь на мгновение, глубоко вздохните, подумайте и перезагрузитесь.

«Безопасность ребенка в Интернете. Памятка для родителей»

Современные дети значительно отличаются от детей не только прошедшего столетия, но и последних десятилетий. Теперь дети стали реже гулять, меньше общаться со сверстниками, предпочитая виртуальных друзей. Привычные возгласы мам "Опять на улицу собрался?!" сменились не меньшими по эмоциям "Опять в Интернете сидишь?!". К сожалению, это реалии времени, с которыми необходимо считаться. Интернет все больше вторгается в нашу жизнь. И дети начинают с ним знакомство порой в очень раннем возрасте.

Виртуальное пространство – увлекательный мир, его возможности безграничны. Но Сеть таит в себе много опасностей, неискушенное чадо может быть очень легко обмануто, его доверие несложно завоевать посредством Интернета даже при помощи обычной переписки. Этим, как правило, и пользуются киберпреступники. Чтобы обезопасить юного пользователя от возможных бед, надо провести подробный инструктаж перед тем, как он начнет осваивать киберпространство.

Первое. Расскажите ребенку, что представляет собой Интернет-пространство, чем полезен Интернет, что можно там найти интересного и что негативного можно встретить. Лучше представить виртуальную сеть как помощника в поиске информации или как средство образования, а не как возможность для развлечений и удовольствий, чтобы ребенок не просиживал все свободное время в сети, а правильно распределял его по необходимости.

Второе. Договоритесь с ребенком, сколько времени он будет проводить в сети. Для каждого возраста должно быть свое время – чем старше ребенок, тем больше он может находиться в сети, но определенные рамки все равно должны

сохраняться. Десятилетнему ребенку достаточно и 30 минут. Можно создать список домашних правил пользования Интернетом, где будет указан перечень сайтов, которые можно посещать, информация о защите личных данных, этика поведения в сети и прочее.

Третье. Предупредите свое чадо о том, что в сети он может столкнуться с запрещенной информацией и злоумышленниками. Речь идет о насилии, наркотиках, порнографии, страницах с националистической или откровенно фашистской идеологией. Ведь все это доступно в Интернете без ограничений. Часто случается так, что просмотр подобной информации даже не зависит от ребенка – на многих сайтах отображаются всплывающие окна, содержащие любую информацию, чаще всего порнографического характера. При столкновении с негативным контентом, ребенок обязательно должен рассказать об этом родителям.

Четвертое. Приучите детей к конфиденциальности. Если на сайте необходимо, чтобы ребенок ввел имя, помогите ему придумать псевдоним, не раскрывающий никакой личной информации. Расскажите детям о том, что нельзя сообщать какую-либо информацию о своей семье – делиться проблемами, рассказывать о членах семьи, о материальном состоянии, сообщать адрес.

Пятое. Беседуйте с детьми об их виртуальных друзьях и о том, чем они занимаются так, как если бы речь шла о друзьях в реальной жизни. Часто педофилы регистрируются на детских сайтах, вступают в переписку с ребенком, общаются длительное время – все это для определенной цели – завоевать доверие ребенка и добиться встречи с ним. Каковы могут быть последствия встречи, догадаться несложно. Приучите детей рассказывать о встречах в реальной жизни. Если ребенок хочет встретиться с другом, он обязательно должен сообщить об этом взрослым.

Шестое. Расскажите о мошенничествах в сети – розыгрышах, лотереях, тестах, чтобы ребенок никогда, без ведома взрослых, не отправлял смс, чтобы узнать какую-либо информацию из Интернета.

Седьмое. Объясните детям, что никогда не следует отвечать на мгновенные сообщения или письма по электронной почте, поступившие от незнакомцев. Если ребенка что-то пугает, настораживает или кто-то угрожает в переписке, в письме, он обязательно должен сообщить об этом взрослым.

Ознакомьте ваше чадо с этими простыми правилами, и он будет иметь представление о том, с чем может столкнуться в Интернете, и будет знать, как вести себя в этом случае. Если ребенок будет вам доверять и рассказывать все, что впечатлило его в сети, с кем он познакомился, вы сможете избежать очень серьезных бед, таких как похищение ребенка посредством сети и сексуальная эксплуатация детей. Но не переборщите – не надо запугивать ребенка Интернетом, говорить, что это очень опасная и страшная штука, но ей надо уметь пользоваться. Ребенок должен усвоить мысль, что Интернет – это друг, и если правильно с ним «дружить», можно извлечь из этого очень много пользы. А правильно «дружить» с ним научить может только взрослый. Так что все карты вам в руки.