МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Гуманитарно-педагогический институт
(наименование института полностью)

Кафедра «Социология»
(наименование кафедры)

39.03.01 Социология
(код и наименование направления подготовки, специальности)

БАКАЛАВРСКАЯ РАБОТА

на тему «Обеспечение информационной безопасности в российском современном обществе»

Студент Г.С. Назришоева _____
(И.О. Фамилия) (личная подпись)

Руководитель Т. Н. Иванова _____
(И.О. Фамилия) (личная подпись)

Допустить к защите

Заведующий кафедрой
д-р социол. наук, профессор Т. Н. Иванова _____
(ученая степень, звание, И.О. Фамилия) (личная подпись)
«_____»_____20_____г.

Тольятти 2019

Аннотация

Объектом данной бакалаврской работы является функционирование информационного общества, предметом – информационная безопасность общества и личности в условиях модернизирующегося общества.

Целью данной работы является анализ функционирования и методов обеспечения информационной безопасности в современном Российском обществе.

Структура работы. Данная работа состоит из введения, двух глав (четырёх параграфов), заключения, списка литературы и источников, приложений

В первом параграфе первой главы мы рассмотрели труды зарубежных и отечественных ученых, занимавшихся информационным обществом как Д. Белл, М. Кастельс, Э. Тоффлер, К. Ясперс, Ю. Хабермас и Э. Гидденс.

Во второй главе мы рассмотрели проблему информационной безопасности и подходы к ее изучению. Значимыми работами были М.И. Дзлиева, К.К. Колина, С.П. Расторгуева, Г.Л. Смоляна, Д.С. Черешкина, В.Н. Лопатина, Т.А. Поляковой, Н.В. Лопатиной.

В первом параграфе второй главы рассмотрено изучение представление об информационной безопасности, полученное при помощи анкетирования жителей г.о. Тольятти.

Во втором параграфе второй главы по результатам индивидуального стандартизированного интервью описаны мнения студентов об различных факторах информационной безопасности.

Оглавление

Введение

Актуальность темы исследования. Современное общество по праву может, называется информационным. Оно обусловлено прогрессом и развитием информационных технологий и связей коммуникации. Информация – одна из основных ценностей человека. Не случайно в оборот вошла цитата «кто владеет информацией, тот владеет миром». Информационные технологии захватили все сферы общественной жизни.

Распространение совершенно новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили уровни защиты информации и вызвали необходимость в том, чтобы эффективность защиты информации росла вместе со сложностью архитектуры хранения данных. Так постепенно защита экономической информации становится обязательной: разрабатываются всевозможные документы по защите информации; формируются рекомендации по защите информации; даже проводится федеральный закон о защите информации, который рассматривает проблемы защиты информации и задачи защиты информации, а также решает некоторые уникальные вопросы защиты информации.

Так, в Доктрине информационной безопасности под таковой понимается «состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства»[1].

Становление информационного общества дало начало развитию информационной преступности, которая может быть направлена против личности, государства и общества. Сюда относятся так называемые компьютерные преступления, направленные на несанкционированный доступ к базам данных автоматизированных информационных систем

[1] Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс] // Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71456224/ (дата обращения: 03.03.2019).

органов государственной власти, финансовых организаций и промышленных корпораций. В этих системах в процессе информатизации общества накапливается большое количество конфиденциальной информации о деятельности соответствующих организаций, а также данных персонального характера о гражданах страны, их адресах, телефонах, имуществе, доходах. Эта информация представляет значительный интерес для преступных группировок.

Новым явлением в области информационной преступности является информационный терроризм, в результате которого функционирование той или иной информационной системы может быть практически парализовано. Чаще всего это происходит в результате специально организованных массированных сетевых атак, которые в последние годы наблюдались неоднократно с использованием возможностей сети Интернет[2].

Таким образом, проблема информационной безопасности общества на сегодняшний день стоит крайне остро и нуждается в тщательном изучении. Она связана с защитой интересов страны и народа в социальной сфере, развитием социальной структуры и общественных отношений, системы жизнеобеспечения, социализации людей, образа жизни и соответствующего потребностям прогресса нынешних и будущих поколений.

Важнейшим мероприятием, направленным на обеспечение информационной безопасности, наряду с развитием законодательства и систем обеспечения контроля в данной сфере является развитие информационной культуры населения, поскольку, прежде всего, информационная безопасность каждого человека зависит от его собственных умений «фильтровать» потребляемую им информацию.

Степень научной разработанности темы. Информационную безопасность изучали ряд отечественных и зарубежных ученых. Зарубежные

[4] Колин К.К. Гуманитарные проблемы формирования информационного общества // Вестн. Кемеров. гос. ун- та культуры и искусств. – 2010. – № 12. – С. 8- 19.

ученые как Д. Белл, М. Кастельс, Э. Тоффлер, К. Ясперс, Ю. Хабермас и Э. Гидденс рассматривали информационное общество.

Среди отечественных ученых, внесших значительный вклад в развитие этого направления, следует выделить И.Н. Курносова, В.М. Глушкова, А.И. Ракитова.

Проблема информационной безопасности рассматривается в работах целого ряда отечественных исследователей М.И. Дзлиева, К.К. Колина, С.П. Расторгуева, Г.Л. Смоляна, Д.С. Черешкина, В.Н. Лопатина, Т.А. Поляковой, Н.В. Лопатиной и других.

Цель бакалаврской работы – анализ функционирования и методов обеспечения информационной безопасности в современном российском обществе.

Объектом исследования является феномен информационного общества.

Предмет исследования – информационная безопасность общества и личности в условиях модернизирующегося общества.

Задачи исследования:

1) Рассмотреть основные теоретико-методологические подходы к изучению информационного общества и информационной безопасности;

2) Выявить способы обеспечения информационной безопасности;

3) Определить степень оснащенности населения города Тольятти по информационной безопасности.

4) Проанализировать уровень удовлетворения политикой информационной безопасности современного российского общества.

Гипотеза исследования. В рамках быстроменяющегося и развивающегося информационного общества весомую роль занимает обеспечение информационной безопасности.

Теоретико-методологическая база исследования:

Постиндустриальный подход (Д.Белл, М.Кастельс) позволит рассмотреть информационное общество как базис информационной безопасности.

Рисковый подход (У. Бек) позволяет рассмотреть мотивы зарождение информационной безопасности.

Технологический подход позволяет рассмотреть информационную безопасность в современном технологическом обществе.

Феноменологический подход данный подход позволяет изучить восприятие информационной безопасности в современности

Методы исследования: анкетный опрос (100 респондентов), глубинное интервью (10 респондентов).

Эмпирическая база исследования. Анкетный опрос N=100 респондентов (50 респондентов школьники в возрасте 14-18 лет и 50 респондентов студенты в возрасте 19-24 лет). Глубинное интервью N=10 человек (5 студентов гуманитарных специальностей и 5 студентов технических специальностей).

Структура бакалаврской работы. Работа состоит из введения, двух глав (четырех параграфов), заключения, списка используемой литературы и источников, приложений.

Глава 1. Теоретико-методологические основы изучения информационной безопасности общества и личности

1.1. Феномен информационного общества в трудах российских и западных ученых

Настоящее время призвано назваться информационной эпохой. Информация и ее специфические составляющие набирают все большую ценность и значимость. Распространение Изучение информационного общества позволит выявить новые актуальные проблемы и пути их решения. В современном обществе, наполненном угрозами и рисками, особую значимость приобретает безопасность жизнедеятельности и ее составляющая информационная безопасность.

Изучение информационной безопасности начинается со становления информационного общества. Существует множество различных подходов, определяющих понятие «информационное общество». Рассмотрим несколько из них. Дэниэл Белдл, крупнейший теоретик «постиндустриального общества» (этот термин он использует как синоним термина «информационное общество»), предполагает, что мы вступаем в информационное общество, когда большинство занятых работает в информационной сфере. В своей работе «Социальные рамки информационного общества» он определяет сущность нового общества через изменения, происходящие в обществе настоящем, тем самым, выделяя и подчёркивая именно те признаки, которые будут отличать «послереволюционное» общество от сегодняшнего. Три аспекта постиндустриального общества особенно важны для понимания телекоммуникационной революции:

1) переход от индустриального к сервисному обществу;

2) решающее значение кодифицированного теоретического знания для осуществления технологических инноваций;

3) превращение новой «интеллектуальной технологии» в ключевой инструмент системного анализа и теории принятия решений.

В целом Д. Белл определяет постиндустриальное общество как общество, в котором производство сменяется непрерывным воздействием на окружающую среду, а каждая сфера человеческой деятельности тесно связана со всеми другими. Это общество, в котором господствует сервисная экономика, причём быстрее растёт число сервисных работников, связанных с системой здравоохранения, образования, управления. Автор называет в числе основных характеристик такого общества – центральную роль теоретической науки, создание новой интеллектуальной технологии и рост класса носителей знания.

Английский социолог Энтони Гидденс скептически относился к самой идее информационного общества. С его точки зрения, сегодня мы живём в эпоху «радикальной модернизации», отмеченной масштабным проявлением особенностей, которые присущи современному обществу. Он утверждает: «Хотя обычно предполагают, что мы только вступаем в новую эпоху информации, на самом деле современное общество было «информационным» с самого своего начала»[3]. Э. Гидденс приходит к выводу, что значение, которое мы приписываем информации, она имела уже в далеком прошлом, а то, что сегодня информация приобрела ещё большую ценность, не повод, чтобы говорить о возникновении новой системы, на чём настаивал Дэниел Белл, вводя понятие постиндустриального общества. Таким образом, Э. Гидденс считает, что в современном обществе произошла «информатизация» социальных связей с помощью информационных технологий, но это не значит, что мы приближаемся к новому «информационному обществу».

Испанский социолог Мануэль Кастельс считает, что «информационная эпоха» возвещает появление «нового общества», которое возникает благодаря развёртыванию сетей и в котором приоритетное значение имеют

[3] См.: Гидденс Э. Последствия современности. М.: Праксис, 2011. – С.124-125.

информационные потоки. М. Кастельс никогда прямо не говорит о возникновении информационного общества. По его мнению, все общества использовали информацию, и соответственно термин «информационное общество» не имеет большой аналитической ценности для определения особенностей наступившей эры. М. Кастельс доказывает, что мы переживаем переход к «информационной эпохе», главной чертой которой становятся сети, связывающие между собой людей, институты и государства. Это вызывает множество последствий, но самое значительное – возможное усугубление разрыва между возрастающей глобальной деятельностью и обострившимся социальным разделением. М. Кастельса интересуют обе стороны вопроса, он хочет исследовать и способы, которыми глобализация усиливает интеграцию людей и различных процессов, и связанную с ней фрагментацию и дезинтеграцию. Учёный полагает, что включенность в сеть – условие полноценного участия в жизни современного общества. Тем самым утверждается, что доступ к интерактивным информационно-коммуникационным технологиям и, в первую очередь к Интернету, определяет право гражданства в информационной эпохе. Мануэль Кастельс всё же опасается, что если во главе такого общения станет развлечение, то это будет означать, что люди не сами будут поддерживать интерактивное общение, его будут направлять централизованные силы. Более того, Мануэль Кастельс доказывает, что «ценой за включение в систему станет требование адаптации к её логике, её языку, её «проходному баллу», её кодировке и декодировке».

По мнению М. Кастельса, информациональное общество отличается от индустриального тем, что оно стремится не к производству товарной массы из всех доступных сырьевых источников, а к богатству знаний, черпаемых из информационных ресурсов, в целях максимального использования высокоразвитой техники для удовлетворения запросов её пользователей. Если «индустриализм ориентирован на экономический рост, то есть на максимальный выпуск продукции», то «информационализм направлен на

накопление знаний и к более высоким уровням сложности обработки информации»[4].

Отечественные учёные определяли информационное общество как следствие процесса информатизации. Особенно ярко это проявлялось в работах А.И. Ракитова. Советский учёный писал, что переход к информационному обществу предполагает превращение производства и использование услуг и знаний в важнейший продукт социальной деятельности, причем удельный вес знаний будет постоянно возрастать. Главной целью информационного общества, по мнению А.И. Ракитова, является обеспечение правовых и социальных гарантий того, что каждый гражданин общества, находящийся в любом месте и в любое время, сможет получить всю необходимую для решения насущных проблем информацию[5].

И.Н. Курносов считает, что в информационном обществе преобладают удалённые коммуникации, дистанционная работа и досуг, а также формируются новые отношения между людьми в процессе производства и общественной деятельности. Значительная часть ВВП производится в информационном секторе, труд большей части людей становится по характеру информационным, осуществляется развитие интерактивных информационно- коммуникационных технологий, глобальных компьютерных сетей, комплексной обработки представления информации. Представляются новые коммуникационные возможности для взаимодействия и выражения политической воли общества и социальных групп, а также возрастает роль стран с мощным информационным потенциалом[6].

Несмотря на существующие подходы, очевидно, что и информационные и постиндустриальные концепции описывают единую реальность, в качестве которой выступает общество, ориентированное на знание и информацию как основной производственный ресурс. Таким образом, можно определить

---

[4] См.: Кастельс М. Информационная эпоха: экономика, общество и культура / Пер. с англ. под науч. ред. О.И. Шкаратана. – М.: ГУ ВШЭ, 2000. – С.248-250.

[5] См.: Ракитов А.И. Информация, наука, технология в глобальных исторических изменениях. М.: РАН. Институт научной информации, 1998. – С.100.

[6] См.: Курносов И.Н. Роль государства в формировании информационного общества в России // Вестник РФФИ. – 1999. – № 3. – С. 15.

информационное общество, как общество, основой развития которого становится не материальное производство, а производство знаний и информации на базе передовой информационной технологии. Информативность означает, что во всех сферах жизнедеятельности человека определяющие действия предпринимаются на основе информационных технологий; такие определяющие действия организованы в глобальном масштабе в информационные сети и сосредоточены на обработке информации[7].

Информатизация экономики или сферы общественной жизни – это насыщение видов человеческой деятельности информационными технологиями. Степень информатизации становится в настоящее время главным критерием развитости общества, поскольку без использования гигантских массивов информации, без соответствующим образом подготовленных информированных специалистов, без огромных информационных ресурсов невозможно принятие решений в любой области и на любом уровне[8].

В настоящее время люди все чаще подвергаются воздействию различного рода рисков: экономических, природных, политических, техногенных и других. В рамках информационного общества выявляются различные социальные риски. Несмотря на плотность социальных взаимодействий, в обществе наглядны изоляционные тенденции, которые можно интерпретировать в контексте проблемы социального одиночества. Это один из парадоксов информационного общества, так как его принято определять, как общество с высокой плотностью связей. Однако эта высокая степень плотности связей и отношений сопряжена с их поверхностностью. В результате этого чувство одиночества оказывается практически встроенным

[7] См.: Костина А.В. Культура информационного общества: тенденции и противоречия развития // Вестник Рязанского государственного университета им. С.А. Есенина. – 2009.– № 24. – С.72- 98.
[8] Блусь П.И. Информатизация общества как фактор повышения качества жизни населения // ARS ADMINISTRANDI. – 2015. – № 3. – С. 5- 18.

в структуру мира, что приводит к формированию максимально изолированного «Я»[9].

Французский социолог Жан Бодрийяр пишет: «Информации становится всё больше, а смысла всё меньше». В эпоху постмодернизма мы оказались в такой ошеломляющей паутине знаков, что они утратили свою знаковость. Эти знаки поступают с разных сторон, они различны, они быстро меняются, противоречат друг другу, и в результате их способность означать потускнела. Кроме того, аудитория теперь креативна, обладает самосознанием и рефлексией и все новые знаки встречает скептически и насмешливо, а потому легко извращает, переинтерпретирует и преломляет их первоначальный смысл. Поскольку знание, полученное через непосредственный опыт, утрачивает свои позиции, становится очевидным, что знаки больше не представляют прямо что-либо или кого- либо. Понятие о том, что знак представляет какую-либо «реальность», помимо собственной, теряет достоверность[10]. Ж. Бодрияр указывает на подмену ценнносмтей в современном обществе – симулякрами. В серии работ «Войны в заливе не было» ученый показывает, как определенно поданная информация может способствовать поведению общества.

В информационном обществе человеку постоянно нужно осуществлять переходы из одной информационной системы в другую, так как он находится под постоянной угрозой как физической, так и ментальной дезориентации. Состояние множественности смыслов, ценностей, принадлежащих разным культурам, является психологически весьма тяжёлым для него. Человек постепенно утрачивает прочные основания своей жизни, утрачивает способность осуществлять коммуникацию с другими в рамках реальности и даже утрачивает способность к идентификации. Немаловажными являются социальные риски, связанные с увеличением способов манипулирования общественным сознанием, увеличением возможностей тотального контроля,

[9] Арутюнян М.Л. Риски, обусловленные трансформацией социально- политического пространства в современном информационном обществе // Сборники конференций НИЦ Социосфера. – 2014. – № 33. – С. 9.
[10] См.: Уэбстер Ф. Теории информационного общества. – М.: Аспект Пресс, 2004. – С. 12-15.

а также с риском психологической неадаптированности к технологическому давлению. Манипулирование в информационном обществе приобретает глобальные масштабы[11].

Современный уровень развития технологий настолько способствовал распространению возможностей сбора данных, что в качестве следующего риска можно отметить рост «тотального надзора». Этот «надзор» имеет разноплановый характер: с одной стороны, может подразумеваться обычное наблюдение, технологии которого используются в целях безопасности, предотвращая разного рода криминальное или просто недопустимое поведение и действия в публичных или частных местах[12]. В этом случае контроль, безусловно, оправдан. Однако подобного рода «наблюдение», которое время от времени более соотносимо со «слежкой», часто начинает затрагивать практически все стороны общественной жизни. Это, в свою очередь, может привести к формированию общества тотального контроля[13].

Следующим не менее угрожающим социальным риском можно считать нарастающую зависимость общества от техники, Интернета, Социальных сетей и компьютерных игр. В 1995 году американским учёным Айвеном Голдбергом было впервые описано состояние Интернет-зависимости. Учёный определил, что Интернет- зависимость способна вызывать у человека болезненное негативное стрессовое состояние или дистресс. Впервые сам термин «Интернет- зависимость» был также предложен Айвеном Голдбергом, под которой он понимал расстройство поведения в результате использования Интернета и компьютера, оказывающее пагубное воздействие на бытовую, учебную, социальную, рабочую, семейную, финансовую или психологическую сферы деятельности

[11] Сладкова О.Б. Использование информационного мониторинга для манипуляции общественным сознанием // Вестник МГУКИ. – 2005. – Вып. 2. – С. 127.
[12] См.: Васильева М.М. Информационная безопасность России в условиях глобализации // Вестник МГЛУ. – 2010. – № 604. – С. 26- 34.
[13] Арутюнян М.Л. Риски, обусловленные трансформацией социально- политического пространства в современном информационном обществе // Сборники конференций НИЦ Социосфера. – 2014. – № 33. – С. 10.

человека[14]. В качестве основных объектов Интернет- зависимости психолог М.И. Дрепа выделяет: навязчивый серфинг (путешествие в сети, поиск информации по базам данных и поисковым системам); сетевые компьютерные игры; виртуальные знакомства; киберсекс и страсть к онлайновым биржевым торгам и азартным играм[15].

К рискам современного информационного общества также относятся: рост информационной преступности, к которым можно отнести кражи и вымогательства, рост национальных и социальных движений, информационное неравенство. Развитие информационно- коммуникационных технологий сопровождается стремительным развитием глобализации, что приводит к размыванию национальных и политических границ, ускорению темпов индустриализации и унификации культур – частично за счёт образования глобальных конгломератов в области информации, телекоммуникаций и досуга. При интенсивном использовании глобальных сетей возникают новые формы культурной агрессии со стороны наиболее развитых стран в отношении менее развитых, появляется опасность утраты целыми сообществами своей культурной и национальной самобытности, включая самобытность языковую, происходит навязывание человечеству потребительских предпочтений и вкусов в интересах узкой группы транснациональных компаний- производителей[16].

К социальным рискам в информационной среде можно также отнести размывание границ государств, в результате чего происходят элементы утраты национальной самоидентификации. Происходят изменения в семейных отношениях. Процессы коммуникации между людьми облегчаются, меняется пространство коммуникации.

---

[14] Крюкова Е.Н. Интернет- зависимость как один из показателей нарушения межличностных отношений // Вестник Самарского государственного технического университета. Серия: Психолого- педагогические науки. – 2012. – № 1. – С. 87- 92.

[15] Дрепа М.И. Интернет- зависимость как объект научной рефлексии в современной психологии // Знание. Понимание. Умение. – 2009. – № 2. – С.189- 193.

[16] Пищулина Т.В. Специалист в условиях информационного общества // Человек. Спорт. Медицина. – 2008. – № 13 (113). – С. 67- 71.

Вышеперечисленные социальные риски являются главным побудителем возникновения информационной безопасности. Риск, для Ульриха Бека, определяется систематическим взаимодействием общества с угрозами и опасностями, которые порождаются процессом модернизации. Соответственно рисков невозможно избежать, но их минимизировать и управлять является актуальной проблемой для информационной безопасности.

1.2. Показатели информационной безопасности общества и личности

В настоящее время существует явно выраженная тенденция к усилению значимости обеспечения должного уровня информационной безопасности. При этом актуальность проблематики информационной безопасности определяется как переносом акцента в противоборстве различных сторон в информационную область, так и существенным повышением доступности критически важных объектов для различных террористических и деструктивных сил[17]. Глобальные процессы информатизации современного общества и образования также обусловливают существенное обострение проблем информационной безопасности[18].

Информационная безопасность является предметом изучения целого ряда наук, поэтому очень важно рассмотреть различные подходы к определению данного понятия.

Социологический подход к определению информационной безопасности продиктован стремлением рассматривать её как социальную составляющую динамической устойчивой системы, подлежащей сохранению[19]. Любую

---

[17] Пархоменко Н.Г. Выявление угроз информационной безопасности в реальном времени, комплексы контроля информационной безопасности // Известия ЮФУ. Технические науки. – 2003. – № 4. – С. 325- 326.

[18] Юсупов Р.М. Информационная безопасность, кибербезопасность и смежные понятия: CyberSecurity VS Информационной безопасности // Информационное противодействие угрозам терроризма. – 2013. – № 21 (21). – С. 27- 35.

[19] См.: Крапивенский А.С. Социологический и социально- психологический подходы к определению концепта «информационная безопасность» в рекламной коммуникации // Научный вестник Волгоградской академии государственной службы. Серия: Политология и социология. – 2010. – № 2. – С. 53.

информационную технологию, по мнению Н.В. Лопатиной, некорректно рассматривать как внесоциальное явление: «информационная технология, подобно технологии любой природы, выступает продуктом человеческой деятельности., ориентированной на поиск новых инструментов, форм и способов преобразования действительности, удовлетворения социальных потребностей: от потребностей насущных до потребностей развития. Информационная технология – это продукт социального опыта»[20]. Информационная безопасность может быть реализована исключительно в поле общественных отношений и, как любое общественное явление, подлежит социологическому исследованию с целью получения данных о социальной системе (поле функционирования информации) и её реакции как реципиента.

Социально- психологический аспект информационной безопасности обусловлен наличием субъективной стороны восприятия информации индивидами и социальными группами. В контексте информационной безопасности психологическая направленность информационного воздействия осуществляется исключительно в пределах социальной коммуникации и в этой связи затрагивает все виды общественных отношений (политических, экономических, духовных и личностных)[21].

Т.А. Полякова информационную безопасность рассматривает как состояние защищённости национальных интересов Российской Федерации в информационной сфере, состоящих из совокупности сбалансированных интересов личности, общества и государства, от внутренних и внешних угроз, что соответствует принципу обеспечения национальной безопасности в информационной сфере, определенному в Стратегии развития информационного общества в Российской Федерации[22].

---

[20] Лопатина Н.В. Информационные специалисты: социология управления. – М.: Академический Проект, 2006. – С. 97-99.

[21] См.: Крапивенский А.С. Социологический и социально- психологический подходы к определению концепта «информационная безопасность» в рекламной коммуникации // Научный вестник Волгоградской академии государственной службы. Серия: Политология и социология. – 2010. – № 2. – С. 55.

[22] Чеботарева А.А. Информационное право: учеб. пособие. – М.: Юридический институт МИИТа, 2014. – С. 138.

По мнению В.Н. Лопатина, объективно категория «информационная безопасность» возникла с появлением средств информационных коммуникаций между людьми, а также с осознанием человеком наличия у людей и их сообществ интересов, которым может быть нанесен ущерб путём воздействия на средства информационных коммуникаций, наличие и развитие которых обеспечивает информационный обмен между всеми элементами социума. Выделяя отдельно информационно- психологическую безопасность, В.Н. Лопатин трактует её как «состояние защищённости жизненно важных интересов личности, общества и государства от воздействия вредной информации»[23].

Философский подход основывается на выделении трёх составляющих информационной безопасности:

1) удовлетворение информационных потребностей субъектов;
2) обеспечение безопасности информации;
3) обеспечение защиты субъектов[24].

Таким образом, в сущностном плане информационная безопасность, согласно философскому подходу, есть такое состояние объекта, при котором состояние информационной среды, в которой он находится, позволяет ему сохранять способность и возможность принимать и реализовывать решения сообразно своим целям, направленным на прогрессивное развитие. Это означает, что информационная безопасность может достигаться как в результате проведения мероприятий, направленных на поддержание информационной среды в безопасном для объекта защиты состоянии, защиту объекта от деструктивного воздействия, так и путем укрепления иммунитета и развития способности объекта уклоняться от деструктивного информационного воздействия[25].

---

[23] См.: Лопатин В.Н. Информационная безопасность России: Человек, общество, государство. Серия: Безопасность человека и общества.– М.: 2000. – С. 38-50.
[24] См.: Атаманов Г.А. Информационная безопасность: сущность и содержание // Бизнес и безопасность в России. – 2007. – № 47. – С. 108- 114.
[25] Чеботарева А.А. Информационное право: учеб. пособие. – М.: Юридический институт МИИТа, 2014. – С. 135.

Политический подход к пониманию информационной безопасности указывает, прежде всего, на растущую необходимость объединения усилий частного сектора, политических институтов и правоохранительных структур, экспертно- аналитических сообществ в поиске способов противостояния многообразным угрозам в информационной сфере. По мнению политологов Россия всё еще стоит на перепутье, и задача государственной политики в области безопасности РФ состоит не только в том, чтобы защитить граждан и общество от этих угроз, но и реализовать эту политику в таких формах и методах, которые, в свою очередь, не поставили бы под угрозу выбранный демократический вектор развития. Адекватная запросам времени политика в области безопасности должна опираться на приоритеты взаимовыгодного сотрудничества и развития гражданской инициативы, при руководящей и направляющей роли государства. Характерной чертой политической науки стало признание необходимости привлечения к обеспечению информационной безопасности не только институтов федеральной государственной власти, но и структур государственного управления субъектов Федерации[26].

Технический подход основывается, прежде всего, на проблеме разработки требований безопасности сайтов, включающих защиту серверов, лицензирование, сертификацию и аттестацию объектов информатизации, применение криптографических механизмов при передаче данных по каналам связи, использование методов идентификации и аутентификации пользователей на сайте. Кроме того, подчёркивается, что системная работа в сфере правового обеспечения информационной безопасности требует научного обоснования дальнейшей разработки таких нормативных актов, в которых бы в полной мере были учтены международные принципы и нормы, направленные на укрепление международной информационной безопасности и вместе с тем максимально учитывались национальные интересы[27].

[26] Там же, С. 136.
[27] Чеботарева А.А. Информационное право: учеб. пособие. – М.: Юридический институт МИИТа, 2014. – С. 137.

Информационный риск представляет собой определённые и осознанные действия субъекта в информационной сфере, предполагающие возникновение возможных негативных последствий. Примером таких рисков может служить PR- компания или PR- акция, реклама, предвыборная политическая пропаганда, продвижение продукта коммерческой компании на рынок, информационная атака или война в отношении конкурента (противника), внесение в адресные базы важных конфиденциальных данных, работа с новыми, малопроверенныными техническими средствами либо работа на компьютере без надлежащей антивирусной программы. Следует отметить, что информационный риск является проявлением и следствием добровольной и осознанной деятельности самого субъекта в информационной сфере.

В информационной безопасности риск определяется как функция трёх переменных величин:

1) вероятность существования информационной угрозы;
2) вероятность существования незащищённости;
3) потенциальное воздействие[28].

В отличие от информационного риска информационная угроза направлена против интересов субъекта в данной сфере. Информационная угроза, по сути, представляет собой умысел с целью намеренного нанесения вреда субъекту информационной сферы[29]. Учитывая нынешнее развитие информационно- коммуникационных технологий и информационных ресурсов, возрастающее и неуклонное влияние информации на жизнедеятельность личности, общества и государства, а также происходящие процессы глобализации человечества, можно утверждать, что информационные угрозы способны не только воздействовать на информационную безопасность, но также в тех или иных параметрах

[28] См.: Марков А.А. Понятие и характеристика информационных рисков, опасностей и угроз в современном постиндустриальном обществе // Вестник Волгоградского государственного университета. Серия 7: Философия. Социология и социальные технологии. – 2010. – № 1. – С. 125.
[29] См.: Лызь Н.А. Информационно-психологическая безопасность в системах безопасности человека и информационной безопасности государства // Известия ЮФУ. Технические науки. 2014. – Т. 157. – № 8. – С. 58- 66.

оказывать деструктивное влияние на национальную, экономическую, экологическую, социальную и ряд других видов безопасности.

Виды угроз информационной безопасности Российской Федерации обстоятельно представлены в её Доктрине информационной безопасности[30]. С учётом общей направленности Доктрина информационной безопасности Российской Федерации подразделяет угрозы информационной безопасности на следующие виды:

- угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
- угрозы информационному обеспечению государственной политики Российской Федерации;
- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в её продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развёрнутых, так и создаваемых на территории России[31].

В Доктрине информационной безопасности также указано о возрастании масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличении числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и

---

[30] См.: Алексеева Е.В. Доктрина информационной безопасности Российской Федерации как ключевой аспект правового обеспечения национальной безопасности в информационной сфере // Ленинградский юридический журнал. – 2016. – № 4 (46). – С. 97- 103.

[31] Петров В.П., Петров С.В. Информационная безопасность человека и общества: учебное пособие. (Гриф УМО) – М.: Изд- во НЦ ЭНАС, 2007. – С. 234-237.

семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся всё изощрённее.

В настоящее время киберэкстремизм получает всё более широкое развитие[32]. Киберэкстремизм, как форма экстремистской деятельности в информационном пространстве – это криминальное использование технологий приёма, обработки, передачи, хранения и распространения информационных сообщений экстремистского характера, то есть содержащей оскорбления в адрес каких- либо социальных (прежде всего, этнических и религиозных) групп, призывы к насилию над ними[33]. Перед экстремистами в информационной среде раскрываются большие возможности распространения своих взглядов[34]. Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряжённости, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников. В основе различных проявлений экстремизма лежит специфика восприятия человеком информации (её искажением и определённой дозировкой при формировании агрессивной идеологии)[35].

Новая современная проблема, вызывающая необходимость информационной безопасности возникает из-за распространения интернет технологий и социальных сетей на молодую аудиторию. С самых ранних лет

---

[32] Старкова Н.А. Социальные проблемы распространения киберэкстремизма в молодежной среде // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодёжи. Материалы внутривузовской конференции. Под редакцией Г.Н. Чусавитиной, Е.В. Черновой, О.Л. Колобовой. 2015. – Магнитогорск: Магнитогорский государственный технический университет им. Г.И. Носова. – 2015. – С. 419- 427.

[33] Клементьев А.С. Противодействие кибертерроризму и киберэкстремизму: новая сфера правоохранительной деятельности // Противодействие терроризму. Проблемы XXI века. № 2 – М.: ЗАО «Изд- во «Современная экономика и право». – 2013. – С. 25- 30.

[34] См.: Войскунский А.Е. Информационная безопасность: психологические аспекты // Национальный психологический журнал. – 2010. – № 1. – С. 48- 53.

[35] Крапивенский А.С. Подготовка специалистов в сфере информационной безопасности: необходимость гуманитарной эволюции // Вестник ВолГУ. Серия 7: Философия. Социология и социальные технологии. – 2008. – № 2. – С. 197.

происходит интеграция ребенка с цифровым пространством. Молодое поколение с несформированным мировоззрением, взглядами, а также легко поддающемся манипуляции, становится самой уязвимой частью общества. Широко известные программы манипуляции через информационное пространство – «Синий кит», «Момо», «Разбуди меня в 4:20», цель которых было совершение самоубийства подростков. Синий кит – игра, распространившаяся в 2016 году в российских социальных сетях. Подростки в любой социальной сети писали хештеги, по средствам которых с ними связывались кураторы, для установления контакта. Кураторы пользуются поддельными аккаунтами, которые нельзя идентифицировать. Первая часть общения заключается в правилах игра, как никому не рассказывать об игре, всегда выполнять задания, какими они не были, за невыполнение задания выбывание из игры и плохие последствия. Затем на каждый день куратор выдает задания, сначала безобидные, а финальным становится совершение суицида. Момо – женщина с устрашающей внешностью, которая существовала в мессенджере WhatsApp. В процессе общения с данным пользователем, начиналась игра, где нужно исполнять задания, как подняться на крышу, сделать что-то с ножом. При отказе участника от данных действий, начинали приходить угрозы и фотографии смертей. Разбуди меня в 4:20 – игра, по образу похожая на «синий кит», однако сюда попадаю те, кто считает суицид решением всех проблем. С самого начала здесь выдаются задания связанные с болью и жестокостью, которые в последствии способды довести до самоубийства.

Таким образом, информационная составляющая, заложенная в базис любого социально значимого явления, позволяет сделать вывод, что обеспечение информационной безопасности лежит в основе предотвращения важнейших антропогенно- социальных опасностей общества[36]. Информационная безопасность является также важнейшей частью национальной безопасности государства, определяя безопасность его

[36] Там же, С. 198.

социокультурного развития. Основополагающая идея информационной безопасности как социального явления заключается в установлении и реализации морально- этических, нормативно- правовых и организационных отношений между людьми, обеспечивающих сбалансированность интересов человека, общества и государства в информационной сфере[37].

[37] См.: Федорова Ж.В. Информационная безопасность и цензура в современной России: о соотношении понятий // Путь науки. – 2014. – № 5 (5). – С. 75- 77.

Глава 2. Качественные и количественные показатели анализа представлений об информационной безопасности общества

2.1. Исследование представлений об информационной безопасности различных групп молодёжи г.о. Тольятти

В современном быстроразвивающемся обществе человек подвержен множеству рисков. В первую очередь они связаны с информационной средой, где опасность для человека возникает в результате развития Интернета, различных средств массовой коммуникации и информационных систем, которые способны влиять на общественное сознание и даже манипулировать им[38].

Информационное воздействие на личность в условиях растущей глобализации приобретает широкие масштабы. Информационные технологии существенно влияют не только на ценностные установки и поведенческие ориентиры людей, но и на их деятельность[39]. Наиболее уязвимой в этом отношении представляется молодёжь, поскольку молодёжь как особая социальная группа отличается тем, что находится в процессе личностного формирования[40]. Информационные опасности современной молодёжи – это негативная сторона перехода к информационному обществу, формирующееся под воздействием информационных угроз и рисков, которым современный человек должен уметь противостоять, организовывая свою деятельность[41]. В этой связи большое значение имеет процесс формирования у молодёжи особых представлений об информационной безопасности и способности противостоять информационным угрозам в обществе рисков.

---

[38] Емельяненко В.Д. Интернет и ценностно- мировоззренческие основания патриотического воспитания // Новая наука: Теоретический и практический взгляд. – 2016. – № 2- 3 (63). – С. 163- 174.

[39] Емельяненко В.Д. Интернет и ценностно- мировоззренческие основания правосознания//Альманах современной науки и образования. – 2015. – № 7 (97). – С. 66- 70.

[40] См.: Степанищенко О.В. Исследование молодежи как особой социальной группы в социально- гуманитарных науках // Научный журнал КубГАУ- ScientificJournalofKubSAU. – 2011. – № 73. – С. 587- 600.

[41] Богатырева Ю.И. Модель обеспечения информационной безопасности школьников при создании инфобезопасной среды образовательного учреждения // Известия ТулГУ. Гуманитарные науки. – 2013. – № 3- 2. – С. 14- 26.

Целью нашего исследования являлось сравнение представлений об информационной безопасности различных групп молодёжи: первая группа школьного возраста – 14-18 лет, вторая группа – студенты в возрасте 19-24 лет (выборочная совокупность составила 100 респондентов).

Гипотезы исследования были построены на основе сравнения мнений студентов и школьников, поэтому выборочная совокупность представлена в пропорции 50/50.

По половому признаку деление представлено также в равном масштабе, было опрошено 50 юношей и 50 девушек.

Прежде всего, нас интересовало, с какими угрозами информационной безопасности сталкивается молодёжь в своей повседневной жизни, с какой целью обычно использует Интернет, и как вообще выстраивает своё отношение к проблеме информационной безопасности.

Для начала следует узнать, для каких целей молодёжь обычно использует Интернет. Большинство опрошенных используют Интернет для общения в социальных сетях (22%). Студенты и школьники в равной степени выбирали данный вариант (22 и 22%), что показывает одинаковую заинтересованном в сетевом общении молодежи. Общие показатели по вариантам «нахожу нужную информацию», «скачиваю материалы», «пользуюсь электронной почтой» среди всех респондентов относительно равны (19,19 и 17% соответственно). Как выяснилось, вариант «нахожу нужную информацию» чаще всего выбирают студенты (22%), чем школьники (18%), что можно объяснить более высокой потребностью поиска информации для учёбы у студентов. Далее выяснилось, что 10% респондентов чаще всего используют Интернет для того, чтобы играть в сетевые игры. Среди школьников процент выбравших этот вариант в выше (12%), чем среди студентов (8%). Таким образом, можно сделать вывод о том, что Социальные сети для молодёжи различных возрастов являются основным источником получения информации в Интернете, поэтому можно

предположить, что именно в Социальных сетях молодёжь чаще всего может сталкиваться с различными угрозами информационной безопасности.

Поскольку современной молодёжи часто приходится использовать Интернет в своей учебной деятельности, были получены сведения об источниках информации в Интернете, которыми пользуется молодёжь при выполнении учебных заданий. С помощью номинальной шкалы удалось выяснить, что при выполнении учебных заданий более половины респондентов (51%) пользуются бесплатными электронными библиотеками. Этот вариант студенты и школьники выбирали в равной степени по 24% опрошенных. Следующей наиболее выбираемой категорией стал бесплатные сайты с готовыми работами, которую выбрали 37% респондентов. Распределение ответов по возрасту оказалось примерно равным: 18% и 17% среди школьников и студентов соответственно. В равной степени респонденты пользуются электронными библиотеками ВУЗов, сайтами научных журналов, сайтами на которых можно заказать работу (33%, 30%, 32% соответственно). Электронными библиотеками ВУЗов студенты (23%) выбирали значительно чаще, чем школьники (7%). Интересно, что сайтами научных журналов студенты (14%) и школьники (13%) пользуются в равной степени. Реже всего респонденты пользуются платными электронными библиотеками (23%). Лишь 7% опрошенных не пользуются никакими Интернет- источниками при выполнении учебных заданий, где преобладают школьники (6%), чем студенты (1%). Исходя из полученных данных, можно сделать вывод о том, студенты чаще, чем школьники, в своей учебной деятельности пользуются различными Интернет- источниками.

При анализе данных получены сведения о том, как преподаватели относятся к тому, что, выполняя задания, ученики (студенты) используют материалы из Интернета. Около половины опрошенных (49%) отметили, что преподаватели разрешают пользоваться любыми материалами из интернета. Школьников, выбравших данный вариант ответа оказалось больше (56%), чем студентов (42%). Треть опрошенных (32%) отметили, что преподаватели

требуют анализа, обдуманного отношения к материалам, взятым из Интернета. Этот вариант ответа студенты выбирали в два раза чаще (44%), чем респонденты школьного возраста (20%). 18% ответили, что преподаватели запрещают пользоваться любыми материалами из Интернета. В результате выяснилось, что в ВУЗах уровень требований к анализу полученной информации из Интернета гораздо выше, чем в школе.

Информационная безопасность является важнейшим компонентом национальной безопасности. Анкетирование позволило изучить мнения респондентов об угрозах, существующих в информационном пространстве, которые наносят ущерб национальной безопасности страны. 40% ответили, что это пропаганда эгоистических установок и потребительского образа жизни, снижение значимости семейных ценностей. Распределение ответов по возрасту оказалось примерно равным: 17% и 23% среди школьников и студентов соответственно. 39% считают, что провоцирование межэтнической и межконфессиональной напряженности, где школьников и студентов оказалось практически в равном соотношении (21% и 18%). Около четверти опрошенных отмечают такие варианты, как – вовлечение молодежи в асоциальные субкультуры (27%), пропаганда национального превосходства и исключительности (26%), пропаганда сексуальной «распущенности» (24%), рост нарко- и алкогольной зависимости среди молодежи (24%), мошенничество, вовлечение в деятельность финансовых пирамид (26%). Последний, студенты выбирали в три раза больше, чем школьники (19%/7%). В остальные представленных характеристиках молодежь была схожа во мнениях, как и в – размывание традиционной системы ценностей (22% опрошенных), распространение экстремистских взглядов (21%). Вариант – пропаганда насилия и жестокости, который отметило 21 % опрошенных, интересен для исследования тем, что студенты (15%) выбирали его в три раза чаще, чем школьники (6%). Менее популярные варианты как вовлечение в тоталитарные, религиозных секты (16%) и формирование зависимости от азартных игр (11%) имеют существенные различия в ответах респондентов

разного возраста. Студенты отмечали данные варианты значительно чаще (11% и 8%), чем школьники (5% и 3%). 1% опрошенных решили оставить свои ответы в графе «другое». В их числе был такой ответ, как «психологический ущерб». Проанализировав полученные данные, можно сделать вывод о том, что более половины респондентов отмечают высокое значение информационной сферы в составе национальной безопасности.

Интернет занимает немаловажную роль в жизни современной молодёжи. При помощи анкетирования исследованы мнения участников опроса о негативных социальных последствиях распространения Интернета. Мнения респондентов в данном вопросе значительно разделились. Наиболее выбираемым стал «малоподвижный образ жизни» (37%), который студенты (24%) отмечали в два раза чаще школьников (13%). 32% опрошенных считают игроманию и киберзависимость негативным последствием распространения Интернета, влияющим на молодёжь. Этот вариант ответа чаще всего выбирали студенты (19%), чем школьники (13%). Около трети опрошенных в обеих группах отмечают снижение уровня интеллекта (33%), снижение уровня культуры (32%), негативные эмоциональные состояния (31%). Вариант «проблемы, связанные с сексуальным поведением» (27% от общего числа опрошенных) чаще всего выбирали респонденты школьного возраста (17%), чем респонденты в возрасте 19- 24 лет (10%). Одна из основных категорий социальных сетей это возможность к обезличенному и анонимному общению, которые могут рассматриваться как негативное социальное последствие. Данный вариант выбрали 26% респондентов, где студентов (19%), отметивших представленный ответ в три раза больше школьников (7%). Так же студенты (15%) в два раза больше отмечают вариант «пропаганда вредных привычек» (24% от общего числа опрошенных), чем более юная молодежь (9%). Формирование поведения, связанного с риском для жизни (13% от общего числа опрошенных) в равной степени была отмечена молодым поколением (6% школьники, 7% студенты). Менее выбираемый вариант «социальная пассивность, инфантильность»

11%, в четере раза чаще выбирался студентами (9%), чем школьниками (2%). В графе «другое» один респондент указал, что «если человек умный, никаких негативных социальных последствий не будет». Таким образом, удалось выяснить, что студенты в значительной степени отмечают негативные последствия использования интернета, чем молодежь более юного возраста.

При анализе результатов анкетирования получена информация о ситуациях нарушения информационной безопасности, с которыми респондентам приходилось сталкиваться. Выяснилось, что чаще всего респонденты сталкиваются с хищениями логина и пароля (для социальных сетей, электронной почты) (34%). Этот вариант ответа выбрали 19% студентов и 15% школьников. 32 % опрошенных отметили, что сталкивались с вирусными атаками. Данный вариант ответа чаще всего выбирали школьники (18%), чем студенты (14%). Треть опрошенных отметили Вариант «информационное «пиратство» незаконное распространение книг, фильмов» (30%). Так же выяснилось, что распространенной проблемой является спам (29%), с которой больше сталкивались студенты (17%), нежели школьники (12%). Около четверти опрошенных в обеих группах сталкивались с хищение средств с платёжной карты (26%) и нарушение авторских прав (плагиат) (26%). Также выяснилось, что респонденты школьного возраста чаще сталкиваются с хищением персональных данных (9%) и мошенничеством с использованием электронных устройств (12%), чем респонденты в возрасте 19- 24 года (7% и 9% соответственно). Вариант другое выбрал 1% респондентов, где представлена ситуация «использование личных фотографий человека и создание другого аккаунта под именем этого человека». Лишь 10% респондентов никогда не сталкивались с различными нарушениями информационной безопасности. Таким образом, наиболее распространёнными в информационном пространстве угрозами, с которыми приходится сталкиваться молодёжи, являются распространение спама, вирусные атаки, хищение логина и пароля (для социальных сетей, электронной почты).

В результате анализа данных анкетирования удалось выяснить, с какими явлениями в Интернете чаще всего приходит сталкивается молодёжи. Большинство респондентов ответили, что чаще всего при использовании Интернета им приходится сталкиваться с оскорблениями, употреблениями нецензурных слов, выражений (69%). Интересно, что студенты (82%) чаще сталкивались с подобным, чем школьники (56%). Студенты (70%) сталкивались с навязчивыми предложениями знакомств в социальных сетях, «письмами счастья», значительно чаще школьников (56%). 64% респондентов приходилось сталкиваться с фото и видео порнографического содержания. Более половины респондентов (58%) сталкивались в Интернете с информационным насилием, жестокими видеосюжетами, запугивающими, угрожающими кадрами. Около трети опрошенных в обеих группах отметили что сталкивались с проблемами физического наказания (32%), шантажом, принуждением к чему-либо (32%) и побуждением к курению, употреблению алкоголя, жестоким или опасным действиям (36%). Исходя из полученных данных, можно сделать вывод о том, что молодёжи на сегодняшний день довольно- таки часто приходится сталкиваться в Интернете с различными негативными явлениями, в особенности с оскорблениями и навязчивыми знакомствами в Социальных сетях.

На сегодняшний день, пожалуй, одной из самых важных проблем в сети Интернет является проблема «Интернет- пиратства», которая тесно связана с сопутствующей проблемой – нарушением авторского права. С помощью анкетирования удалось выяснить, как респонденты относятся к этому явлению. Треть опрошенных (32%) положительно относятся к «Интернет- пиратству» и считают, что это позволяет получить бесплатный доступ к играм, книгам, фильмам, музыке. Студенты (42%) отмечали данный вариант в два раза чаще, чем школьники (22%). Совершенно противоположная обстановка наблюдается при ответе на вариант «отрицательно, это нарушение закона», где чаще отмечают школьники (46%), чем студенты (20%). В равной степени были отмечены варианты, как

«скорее, положительно. Это вынужденное средство. Лицензионный доступ стоит дорого» (14%) и скорее, отрицательно это нарушает права тех, кто владеет лицензией (21%).

Нельзя отрицать тот факт, что Интернет таит в себе много угроз, с которыми необходимо бороться. На сегодняшний день существуют различные средства и способы противодействия этим угрозам. Респондентам был задан вопрос: «Какими средствами обеспечения информационной безопасности Вы пользуетесь?». Большинство опрошенных (58%) используют антивирусные программы для обеспечения своей безопасности в информационной среде. 36% – антиспамовыми фильтрами, 32% – средствами идентификации и электронными ключами, 23% – межсетевыми экранами, 19% – средствами авторизации. Один респондент в графе «другое» указал, что использует блокировку рекламы на сайтах и программу ghost (чтобы сайты не отслеживали), и один ответил, что не используют никакие средства обеспечения информационной безопасности.

На вопрос: «Кто, по Вашему мнению, должен заниматься обеспечением информационной безопасности?» две трети респондентов (69%) в обеих группах ответили, что каждый человек должен сам заботиться о своей информационной безопасности. 16% респондентов считают, что обеспечением информационной безопасности должны заниматься специальные государственные службы. 15% опрошенных затруднились ответить на этот вопрос. Исходя из полученных данных, можно сделать вывод о том, что молодёжь скорее осознаёт свою личную ответственность за обеспечение своей информационной безопасности, чем пытается перенести её на государственные службы.

В результате анкетирования, было выяснено, как молодёжь относится к различным мерам, предпринимаемым государством для обеспечения информационной безопасности. Респондентам было предложено оценить по пятибалльной шкале (5 – высокая эффективность, 1 – низкая эффективность, 0 – затрудняюсь ответить) эффективность следующих мер обеспечения

информационной безопасности: «информирование молодёжи о правовых актах, обеспечивающих безопасность в информационной сфере» (4,6), «работа государственных и правоохранительных органов по профилактике преступлений в информационной среде» (4,1), «раскрытие преступлений, связанных с использованием информационных технологий» (3), «ограничение доступа молодёжи к информационным ресурсам, представляющим опасность» (3,8), «формирование информационной и коммуникативной компетентности молодёжи» (3,9).

При помощи анкетирования удалось определить степень информированности молодёжи о тех или иных средствах обеспечения государством информационной безопасности (Информирован хорошо – 3; Информирован недостаточно – 2; Не информирован – 1). Как выяснилось, больше всего респонденты осведомлены о запрете на пропаганду террористической деятельности (2,64), а также о защите персональных данных (2,42). Менее всего респонденты в обеих группах информированы о разработке нормативно- правовых актов по обеспечению информационной безопасности (1,88), о государственном контроле (контроле почтовых отправлений, телеграфных и иных сообщений, прослушивание телефонных переговоров при осуществлении оперативно- розыскных мероприятий) (2,13) и о защите прав на собственное изображение (2,15).

Чтобы уметь обеспечивать свою безопасность в информационной среде, необходимо обладать определёнными знаниями. При помощи анкетирования изучены мнения респондентов о мерах повышения информационной безопасности молодёжи. Большинство опрошенных отметили, что знания о факторах, угрожающих жизни и здоровью (60%). Молодежь в возрасте 14-18 (37%) лет чаще выбирала данный вариант, чем молодежь 18-24 (23%). Также в обоих группах высоко отмечали знания о правах личности (59%). Более половины респондентов в обеих группах выбрали вариант ответа «знания о правах личности» (54%) и «о наказаниях за преступления в информационной сфере» (53%). Реже всего респонденты в обеих группах выбирали варианты

ответов «о защите от информации, представляющей опасность для жизни, здоровья» (28%) и «знания о криминальной ситуации» (25%). Полученные данные позволяют сделать вывод о том, что недостаточность знаний в сфере нормативно- правового регулирования и ответственности за преступления в информационной сфере, по мнению респондентов, становятся важнейшим фактором возникновения угроз информационной безопасности.

Две трети опрошенных (76%) считают, что знания о наказаниях за преступления в информационной сфере и о способах защиты прав личности (71%) могли бы поспособствовать повышению информационной безопасности молодёжи. Данные варианты ответов студенты (86% и 76% соответственно) выбирали чаще, чем респонденты школьного возраста (66% в обоих вопросах). Более половины респондентов (57%) выбрали вариант ответа «знания о правах личности», 43% респондентов – «знания о защите от информации, представляющей опасность для жизни, здоровья». Данный вариант ответа респонденты в возрасте 14- 18 лет выбирали гораздо чаще (52%), чем респонденты в возрасте 19- 24 лет (34%). Реже всего респонденты в обеих группах выбирали варианты ответов «знания о факторах, угрожающих жизни, здоровью» (28%) и «знания о криминальной ситуации» (25%). Полученные данные позволяют сделать вывод о том, что недостаточность знаний в сфере нормативно- правового регулирования и ответственности за преступления в информационной сфере, по мнению респондентов, становятся важнейшим фактором возникновения угроз информационной безопасности.

При помощи анкетирования удалось выяснить, как молодёжь оценивает эффективность мер, предпринимаемых государством для обеспечения информационной безопасности. Более половины респондентов в обеих группах (66% школьников и 58% студентов) оценивают меры, предпринимаемые государством для обеспечения информационной безопасности как эффективные (58%). Практически четверть опрошенных (22%, студенты 20% и школьники 20%) оценили их как «недостаточно

неэффективные», также 11% респондентов затруднились ответить на заданный вопрос, в основном школьники 12%. Лишь 9% респондентов в обеих группах оценили меры, предпринимаемые государством для обеспечения информационной безопасности, как «неэффективные», в основном студенты (14%). Исходя из полученных данных, можно сделать вывод о том, что молодёжь в целом склонна положительно оценивать меры, предпринимаемые государством для обеспечения информационной безопасности.

В результате исследования выяснилось, что молодёжи на сегодняшний день очень часто приходится сталкиваться с различными угрозами информационной безопасности в Интернете. Нельзя не отметить, что на сегодняшний день актуальной является проблема принуждения подростков в Социальных сетях к различным действиям, наносящим вред здоровью или жизни. Также стало известно, что школьникам чаще, чем студентам приходится сталкиваться с такими угрозами информационной безопасности, как вирусные атаки, хищение персональных данных и мошенничество с использованием электронных устройств. Таким образом, возрастает необходимость формирования навыков обеспечения безопасности личных данных у современной молодёжи ещё со школьной скамьи. Как выяснилось, учителя менее требовательны к какому- либо анализу информации, полученной в Интернете, при выполнении учебных заданий, чем преподаватели в ВУЗах. Можно предположить, что именно этот фактор может влиять на отсутствие у школьников способности к критическому восприятию и анализу информации в сети Интернет.

2.2. Сравнение мнений студентов-гуманитариев и студентов-программистов о различных факторах информационной безопасности

Помимо анкетирования в ходе исследования было проведено интервью. Оно носило характер индивидуального, проводилось с использованием заранее составленного списка вопросов.

В интервью приняли участие студенты г.о. Тольятти:

Петренко Артём Александрович – студент Института права ТГУ (21 год);

Саяпина Александра Юрьевна – студентка Гуманитарно-педагогического института ТГУ (21 год);

Петров Александр Олегович – студент Института Физической Культуры и Спорта ТГУ (24 года);

Романова Анастасия Александровна – студентка ГумПИ ТГУ (22 года);

Чеснокова Ирина Витальевна – студентка ГумПИ ТГУ (19 лет);

Ильин Никита Андреевич – студент Факультета информатики и телекоммуникаций Волжского университета им. В.Н. Татищева (22 года);

Шелепин Виталий Игоревич – студент Факультета информатики СНИУ, учится заочно, проживает в Тольятти (18 лет);

Зидыганова Елизавета Аркадьевна – студентка Института Математики Физики и Информационных Технологий, ТГУ (23 года).

Орлова Алина Дмитриевна – студентка Института Машиностроения ТГУ (19 лет);

Антюшин Антон Владимирович – студент Института Математики Физики и Информационных Технологий, ТГУ (24 года).

На первый вопрос: *«Как Вы будете действовать, если обнаружите, что на Вашем компьютере появился вирус?»* опрашиваемые ответили следующим образом:

Петренко А.А.: «Включу специальную утилиту, удалю вирус, затем поставлю полную проверку компьютера»;

Саяпина А.Ю.: «Скорее всего, я буду искать решение у знакомых и друзей, либо искать ответ на это в самом Интернете. Удалю все подозрительные файлы»;

Петров А.О.: «Попробую запустить антивурус, если не получится, то отнесу в сервис»;

Романова А.А.: «Если на моем компьютере уже установлен антивирус, то сразу ставлю на проверку и удаляю вирусы, если нет, то скачиваю любую демо-версию антивируса и продолжаю в том же порядке»;

Чеснокова И.В.: «Постараюсь вылечить его при помощи антивирусных программ»;

Ильин Н.А.: «Использую антивирус, для удаления вредоносной программы»;

Шелепин В.И.: «Я буду делать одновременно три вещи: запущу антивирус на быструю, а затем полную проверку; попытаюсь с предельной осторожностью устранить и\или замедлить этот вирус сам, используя собственные знания; найду всю возможную информацию о нем в интернете».

Зидыганова Е.А.: «Скачаю антивирус или блокираторы вируса»;

Орлова А.Д.: «Буду использовать все известные методы для удаления вируса, на самый крайний вариант отдам друзьям-программистам»;

Антюшин А.В.: «Я бы сначала воспользовался антивирусом на проверку, если он нашел данный вирус нажму кнопку вылечить, если не нашел, то посмотрю, что пишут в интернете».

В результате выяснилось, что все респонденты обладают определёнными навыками защиты своих данных на компьютере.

На вопрос: *«Пользуетесь ли Вы торрент-трекерами, если да, то для каких целей?»* респонденты ответили:

Петренко А.А.: «Да, для скачивания и просмотра фильмов, игр, установки различных программ»;

Саяпина А.Ю.: «Пользуюсь. В основном, я скачиваю фильмы и сериалы в хорошем качестве. Реже использую для скачивания дискографий»;

Петров А.О.: «Не использую торрент-трекеры, мне это не за чем»;

Романова А.А.: «Периодически пользуюсь. Раньше больше, так все было проще, а последнее время только сериал «Игру Престолов» скачивала, так как ее везде блокировали,а посмотреть то хочется»;

Чеснокова И.В.: «Использую иногда, когда нужно скачать на компьютер что-либо, но последнее время очень мало»;

Ильин Н.А. ответил, что не пользуется торрент- трекерами;

Шелепин В.И.: «Да, я пользуюсь торрент- трекерами, так как это, как ни странно, наиболее безопасный способ скачивания чего- либо в интернете, после официальных ресурсов конечно. В основном я использую их для скачивания иностранных сериалов и бесплатно распространяемого ПО, иногда для неофициального программного обеспечения (неофициальное ПО ≠ нелицензионное ПО). Под оф. ресурсами я подразумеваю сайты фирм и организаций, гос. системы, сайты разработчиков ПО, все остальные потенциально небезопасны для скачивания»;

Зидыганова Е.А.: «Да, пользуюсь, но иногда, только для скачивания фильмов, хотя годиков семь назад, скачивала игры на компьютер»;

Орлова А.Д.: «Пользуюсь, скачиваю сериалы, чтобы потом смотреть на телевизоре»;

Антюшин А.В.: «Да, пользуюсь, но только для того, чтобы скачать фильмы для поездок, где не будет интернета».

Таким образом, выяснилось, что только два респондента не пользуются торрент- трекерами, где преимущественно распространены файлы, нарушающие закон об авторском праве.

Благодаря следующему вопросу, мы узнали, *как респонденты относятся к блокировке торрент-трекеров:*

Петренко А.А.: «Отрицательно, но я обхожу их, так что в целом мне всё равно»;

Саяпина А.Ю.: «Отрицательно, хоть и понимаю, по какой причине их запрещают. При блокировке торрента я ищу либо новый торрент- трекер, либо ссылку на «зеркало» закрытого торрента»;

Петров А.О.: «Негативно, я в принципе отношусь плохо к пиратству»;

Романова А.А.: «Я против их блокировки, ведь есть люди, которые не могут позволить себе часто ходить в кинотеатр, а фильм хочется посмотреть»;

Чеснокова И.В.: «Мне не нравится, что теперь нет открытых торрент доступов, стало очень затруднен поиск фильма или провереного сайта для скачивания. Больше вирусов наберешься»;

Ильин Н.А.: «Отношусь к этому нейтрально, мне достаточно лицензионного/бесплатного контента»;

Шелепин В.И.: «С правовой точки зрения, а если точнее, с точки зрения государства, блокировка торрент- трекеров закономерна. Но тут интересно, в чём заключается вопрос? Как я отношусь к новостям, о том, что государство блокирует торрент- трекеры? Я рад, потому что государство наконец начало разбираться и наводить шороху в РуНете, а это важно, ведь наше будущее лежит в информационной среде, её важность, влияние с каждым годом неуклонно возрастает. А может вопрос заключается в том, как я отношусь к тому, что более не имею доступа к заблокированным торрент- трекерам? На самом деле тема с торрент- трекерами наиболее популярна в РуНете потому что, любой самый неопытный пользователь ПК имел доступ к огромной базе «всего», и что самое главное, брать он мог это «всё» бесплатно. Но, допустим, такого доступа нет, что же, этот пользователь пойдет в магазин, и купит, всё то, что ему нужно? Нет, у него нет денег для этого, или его не устраивает соотношение цены и качества. Отвечая на этот вопрос, я могу с уверенностью сказать, что меня никак не волнует блокировка, потому что у меня есть доступ к торрент- трекерам, и будет доступ к торрент- трекерам ещё очень долгое время, так как большое количество пользователей таких ресурсов делают всё, чтобы торрент- трекеры никуда не пропали и любой

имел к ним свободный доступ. Им в этом помогает то, что государство практически не имеет никакого контроля в интернете, а система торрентов основана на том что каждый участник процесса подключает себя к сети, и тем самым делает её более независимой от главного ресурса. В итоге получается, что проще запретить весь Интернет, чем запретить торренты- трекеры»;

Зидыганова Е.А.: «Отношусь нейтрально, нет сильного положительного или отрицательного мнения»;

Орлова А.Д.: «Мне все-равно, так как если потребуется что-либо скачать это можно будет найти в интернете. Бесполезна эта блокировка»;

Антюшин А.А.: «Смотря с какой стороны посмотреть. Конечно для простых пользователей – блокировка торрент-трекеров сказывается негативно, но с другой стороны все правомерно».

В результате выяснилось, что студенты- гуманитарии отрицательно относятся к блокировке торрент- трекеров, в то время, как студенты- программисты относится в целом нейтрально.

Задав вопрос: «*С какими угрозами информационной безопасности Вам приходилось сталкиваться в Интернете?»,* мы получили следующие ответы:

Петренко А.А.: «Взлом аккаунта почтового ящика, с которым были связаны многие интернет- сервисы»;

Саяпина А.Ю.: «С угрозами я практически не сталкивалась. Иногда возникали проблемы со скачиванием «подозрительных» файлов, когда в ходе установки устанавливались «лишние» файлы, рекламные баннеры и прочее. Но с такими проблемами обычно легко было разобраться, используя очистку компьютера с помощью антивируса»;

Петров А.О.: «Не сталкивался с угрозами инйормационной безопасности»;

Романова А.А.: «Были и взломы страниц в социальных сетях, хорошо, что вымогательством денег не закончилось. И вирусы на персональном компьютере»;

Чеснокова И.В.: «Пока еще не сталкивалась с такими угрозами»;

Ильин Н.А. ответил, что не сталкивался с угрозами информационной безопасности;

Шелепин В.И.: «Угроза использования моих личных данных мошенниками, удаления моих личных документов, вымогательство, использование моих технических ресурсов в интересах мошенников»;

Зидыганова Е.А.: «Никакими»;

Орлова А.Д.: «Бывало меня взламывали в социальной сети Вконтакте, достаточно не приятно»;

Антюшин А.В.: «Ну, если расценивать вирус, как информационную угрозу, то да с ними сталкивался».

С помощью следующего вопроса, *удалось выяснить, какую информацию о себе респонденты не стали бы распространять в Интернете*:

Петренко А.А.: «Я в целом стараюсь выкладывать как можно меньше информации о себе, но если выделить что-то одно, то это, конечно же, данные банковских карт, фото документов и т.д.»;

Саяпина А.Ю.: «Я не стала бы распространять информацию, связанную с моей личной жизнью; неудачными моментами, произошедшими, когда- либо; личные фотографии и видеозаписи»;

Петров А.О.: «Свою сексуальную жизнь или достачно близкие и интимные отношения и части тела»;

Романова А.А.: «Если честно, с развитием технологий все становится цифровым. Кредитной картой становится телефон, портал госуслуг вообще всю информацию о тебе знает. А в социальных сетях мы сами все о себе рассказываем».

Чеснокова И.В.: «Не знаю, наверно, паспортные данные и другие документы»

Ильин Н.А.: «Паспортные данные, номера кредитных карт, пароли»;

Шелепин В.И.: «Я бы не стал распространять любую информацию о себе в интернете. Делаю это исключительно из-за необходимости»;

Зидыганова Е.А.: «Свое семейное положение, как говорится счастье любит тишину»;

Орлова А.Д.: «Ничего не распространяю, я инкогнито»;

Антюшин А.В.: «Интимные фотографии, так как сейчас участили взломы страниц и угрозы с шантажем».

Далее последовал вопрос о том, *какие меры респонденты предпринимают для защиты своих данных в Интернете:*

Петренко А.А.: «Я использую на всех своих аккаунтах различные сложносочиненные пароли, ни один из которых не дублируется. Я не скачиваю подозрительные файлы, а также перед запуском каких- либо новых программ, скаченных из интернета или с внешнего носителя, проверяю их на наличие вирусов. Также, я слежу за обновлениями своей операционной системы и антивируса»;

Саяпина А.Ю.: «Если я хочу огородить каких- то пользователей от своих подписок, групп, ссылок на аккаунты, то эту информацию я скрываю либо в настройках приватности в социальных сетях, либо и вовсе не выкладываю ту информацию, которую «боюсь» показать остальным. Раньше использовала в целях безопасности своего компьютера антивирус, сейчас не предпринимаю для безопасности никаких мер, кроме как использования сложных и длинных паролей»;

Петров А.О.: «Стараюсь писать и выкладывать минимум информации и только то, что мне не навредит в любом контексте»;

Романова А.А.: «Стараюсь не заходить и не регистрироваться на подозрительных сайтах. В социальной сети Вконтакте перед каждым использование с компьютера требует помимо стандартного логина и пароля еще и смс пароль»;

Чеснокова И.В.: «Использую антивирус, специальные программы блокаторы и не подключаюсь, через свободный и открытый вай фай»;

Ильин Н.А.: «Использую антивирусы, не выкладываю подробную информацию в свободный доступ»;

Шелепин В.И.: «Стараюсь выкладывать их минимальное количество и доверяю лишь официальным ресурсам, не распространяю личную информацию, даже доверенным лицам через Интернет».

Зидыганова Е.А.: «Использую специальные блокираторы в браузере, также у меня закрытый инстаграмм, я сама выбираю людей, которые будут видеть мои фотографии»;

Орлова А.Д.: «Стараюсь выкладывать только ту информацию, которой невозможно мне навредить»;

Антюшин А.В.: «Я специально создаю большие пароли с различными комбинациями цифр и букв, а также не регистрируюсь на странных и подозрительных сайтах».

В результате удалось выяснить, что все респонденты, независимо от профиля обучения, стараются обеспечивать свою безопасность в информационной среде различными способами. В основном респонденты стараются выкладывать в сеть меньше информации о себе.

Затем последовал вопрос: *«Как Вы относитесь к тому, что специальные службы могут собирать, хранить и просматривать Вашу переписку или любые другие личные данные, в качестве способа обеспечения общественной безопасности?»*, на который респонденты дали следующие ответы:

Петренко А.А.: «Негативно, но я понимаю, что в современных условиях информационного общества ради обеспечения безопасного пользования сетью этого не избежать, так что не обращаю внимания, так как мне по сути нечего скрывать от спецслужб»;

Саяпина А.Ю.: «Отрицательно отношусь к этому. Не считаю, что просмотр личных данных абсолютно всех людей населения может как- то помочь. Думаю, что для того, чтобы ввести закон, направленный против антитеррористических действий, достаточно разрешить доступ к любому, кто

является подозрительным по конкретным пунктам (например, подозреваемый в каком- либо деле). С этим законом получается так, что могут просматриваться и те данные, которые к делам, по которым они, казалось бы, должны работать, имеют мало отношения»;

Петров А.О.: «Отношусь негативно, это посягательство на личную тайну»;

Романова А.А.: «Я плохо к этому отношусь, потому что это мое личное пространство и для обеспечения безопасности это мало поможет. Есть многие мессенджеры, которые невозможно взломать, и я считаю, что это просто перекрытие для обычной отмывки денег»;

Чеснокова И.В.: «Негативно, сейчас когда все через интернет и социальные сети, включая отношения, получается жизнь на показ»;

Ильин Н.А.: «Если это не сказывается негативно на моей личной жизни и является необходимостью для обеспечения безопасности, то нейтрально»;

Шелепин В.И.: «Если они смогут обеспечивать безопасность, то я только за. Однако, если они будут каким- то образом распространять мою личную информацию, то я категорически против, даже если это для обеспечения общественной безопасности».

Зидыганова Е.А.: «Безразлично, мне нечего скрывать, если им интересно чем занимается и о чем разговаривает молодежь. А ведь кому то за это деньги платят»;

Орлова А.Д.: «Пусть слушают и прочитывают мои разговоры, делать им больше нечего»;

Антюшин А.В.: «В современности все люди знают о прослушивании разговоров и прочтении переписок, это уже как обыденно и это не исключить».

Таким образом, студенты- программисты высказали положительное отношение к просмотру их личной информацией специальными службами

при условии её неразглашения, в то время как студенты- гуманитарии высказали своё негативное отношение.

На вопрос: *«Как Вы считаете, какая персональная информация представляет для Интернет-мошенников наибольший интерес?»* респонденты ответили:

Петренко А.А.: «Несомненно, данные банковских карт, мошенников всегда в первую очередь интересует денежная сторона преступления»;

Саяпина А.Ю.: «Думаю, что Интернет- мошенники в первую очередь интересуются информацией о паролях к банковским картам; какую- либо личную информацию, которую можно направить против человека, тем самым шантажируя его; информацию о документах. В редких случаях, по моему мнению, мошенников может интересовать место проживания»;

Петров А.О.: «Паспортные данные и личная переписка, с этими данными можно завоевать человека полнгстью»;

Романова А.А.: «Заполучение денег любым путем, взломы и писать от имени человека или просто похитить данные карты и тому подобное»;

Чеснокова И.В.: «Большинство мошенников используют личную переписку, чтобы обманным путем заработать больше средств или номер карты»;

Ильин Н.А.: «Логины и пароли от электронной почты, виртуальных кошельков»;

Шелепин В.И.: «Личная информация, которую возможно продать. Что ценного из личной информации у вас есть, вы должны знать сами. Личная информация, которая может как- то намекнуть на пароли к вашим аккаунтам, например, дара рождения, или девичья фамилия ваше матери. Если вы медийная или общественная личность, то это материалы, которые помогут скомпрометировать вас»;

Зидыганова Е.А.: «Номер телефона, ведь он привязан ко всему, банковским картам, личным аккаунтам и тд»;

Орлова Д.А.: «Данные банковской карты, ведь мошенников интересуют в основном деньги»;

Антюшин А.В.: «Я считаю, что большинство – это чтение переписок, из которых могут забрать фотографии или что-либо другое компрометирующее, чем в дальнейшем можно угрожать и шантажировать».

На вопрос: *«Насколько Вы доверяете информации, распространённой в Интернете?»*, были получены следующие ответы:

Петренко А.А.: «Я отношусь к любой информации из сети Интернет с критической точки зрения, но в некоторых случаях я всё же доверяю информации из Интернета, составленной на основе количественных оценок (отзывы на различные продукты)»;

Саяпина А.Ю.: «Я доверяю той информации в Интернете, которую считаю проверенной. Таких источников немного. Часто Интернет- СМИ за счет громких заголовков привлекают пользователей, но информацию их статьи и видео содержат либо неверную, либо провокационную. Так как источников, которым я доверяю, немного, то и к большинству информации в интернете я отношусь с презрением»;

Петров А.О.: «На 50% я доверяю информации из интернета, нужн еще уметь фильтровать информацию, отличать ложь от правды»;

Романова А.А.: «Ну в интернете можно найти правильный ответ, просто надо эту информацию перепроверять».

Чеснокова И.В.: «Интернет – это огромная библиотека, где есть хорошие и нужные книги, а есть непроверенные и глупые. Главное тут правильно определить, где как какая»;

Ильин Н.А. ответил, что относится к информации в Интернете с недоверием;

Шелепин В.И.: «На 90% процентов я не доверяю всему, что вижу».

Зидыганова Е.А.: «50 на 50, так скажем. В интернеете ведь выкладываются электронный издании и пособия, которые нужны нам при учебе, то что мы изучаем в университете, этому я доверяю. А вот различным

новостям или сайтам про здоровье нет, там могут понаписать все, что угодно»;

Орлова А.Д.: «Не доверяю интернету, доверяю только близким родным и друзьям»;

Антюшин А.В.: «Не доверяю информации в интернете в плане новостей и центральному телевидению, которые в большинстве своем проводят чисто манипуляторные передачи и программы».

В целом все респонденты высказали своё недоверие к информации, распространённой в Интернете, при этом студенты- гуманитарии отметили, что всё же доверяют некоторой информации.

Далее удалось выяснить, *какие источники информации респонденты считают наиболее достоверными*:

Петренко А.А.: «Больше всего я доверяю всё- таки Интернету, т.к. он ещё не настолько коррумпирован, и в нём всё ещё есть некая свобода слова, в отличии от телевизора или газет»;

Саяпина А.Ю.: «Наиболее достоверным источником я всё же считаю Интернет. Я думаю, что телевидение во многом ограничивает людей от основной, нужной информации, говоря либо то, что выгодно им, либо изменяя новости так, как опять же выгодно им. В Интернете многую информацию можно проверить хотя бы частично»;

Петров А.О.: «Проверенные сайты, в которых убедился на личном опыте»;

Романова А.А.: «В настоящее время, наверно, не существует такого источника, которому можно было бы открыто доверять, однако интернет все-таки, пока не заблокировали, большинство говорит то, что думает, поэтому остается интернет»;

Чеснокова И.В.: «Если рассматривать средства массовой информации, то все-таки интернет источники»;

Ильин Н.А. ответил кратко «не знаю»;

Шелепин В.И.: «Это организации, фирмы и государственные учреждения и их официальные сайты».

Зидыганова Е.А.: «Учебникам и научной литературе, электронным учебным изданиям»;

Орлова А.Д.: «Я доверяю специалистам в той или иной области»;

Антюшин А.В.: «Ну у меня таких попросту нет».

Таким образом, студенты- гуманитарии отметили, что из различных источников информации больше всего всё- таки доверяют Интернету.

На вопрос: *«Как Вы действуете, когда видите рекламу в Интернете? Воспринимаете ли её всерьёз или не обращаете внимания?»* респонденты дали ответы:

Петренко А.А.: «У меня стоит расширение для браузера, блокирующее любую рекламу, в том числе и всплывающую, так что я не сталкиваюсь с этим. В редких случаях, когда я всё- таки вижу рекламу, она вызывает у меня раздражение, и я стараюсь её закрыть и заблокировать»;

Саяпина А.Ю.: «В браузере, которым я пользуюсь, стоят приложения, блокирующие рекламу. Но даже эти приложения не всегда блокируют навязчивую всплывающую рекламу. Обычно такая реклама меня раздражает, и я закрываю те сайты, на которых она навязчива и её не получается скрыть»;

Петров А.О.: «Не обращаю внимания на рекламу, привыкла к ней, она сейчас везде»;

Романова А.А.: «У меня стоит адблок, приложение которое блокирует большинство реклам. А те которые все-равно показывают, я поматываю и не обращаю внимания»;

Чеснокова И.В.: «Бегло просматриваю рекламу, но никогда не захожу, так как не различаю какая реклама обычная, а какая с вирусами»;

Ильин Н.А.: «Не обращаю внимание на рекламу»;

Шелепин В.И.: «Если я вижу рекламу в Интернете, а вижу я её очень редко, так как у меня стоит очень большое количество блокировщиков

рекламы, то я её не воспринимаю как информацию в принципе потому, что доверие к этой информации буквально равно нулю».

Зидыганова Е.А.: «Не обращаю внимания на рекламу, привыкла к ней. Сейчас реклама идет и перед просмотрами видео, и перед входом ан определенные сайты, она везде. И нам нужно научиться просто не обращать на нее внимания, чтобы проще жилось»;

Орлова А.Д.: «У меня стоят несколько блокировщиков рекламы, однако в плеерах, при просмотре видео или музыки она все-равно появляется. Это раздражает»;

Антюшин А.В.: «Я не обращаю на рекламу внимание. Реклама сейчас – это основной источник заработка для разработчиков и программистов, поэтому сейчас она везде и обыденность»

Таким образом, практически все респонденты используют специальные программы, блокирующие рекламу в Интернете, а также относятся к ней с недоверием.

Затем последовал вопрос: *«На Ваш взгляд, распространение какого типа информации в Интернете может оказать негативное влияние на молодёжь?»*, на который респонденты дали следующие ответы:

Петренко А.А.: «Пропагандистские материалы любого характера»;

Саяпина А.Ю.: «По моему мнению, на молодёжь влияет любая информация, призывающая к чему- либо. Это и пропаганда, и агитационные материалы. Не всегда такая информация несет в себе негативную составляющую, но часто воспринимается аудиторией некорректно»;

Петров А.О.: «Порнографии и наркотики»;

Романова А.А.: «Привлечение к негативным действиям, как суицид, то есть это различные игры как «разбуди меня в 4:20», «синий кит», «момо»;

Чеснокова И.В.: «Пропаганда курения, алкоголя, наркотиков и тому подобное, получается не здорового образа жизни»;

Ильин Н.А.: «Пропаганда алкоголя, табачной продукции, наркотиков»;

Шелепин В.И.: «Любого такого же типа, что и не в Интернете, например, экстремистского».

Зидыганова Е.А.: «Игры, такие как Синий кит и разбуди меня в 4:20»;

Орлова А.Д.: «Видео, которые могут в дальнейшем негативно складываться на психике и развитии молодежи»;

Антюшин А.В.: «Новости с непроверенной информацией, я так думаю»;

Таким образом, все респонденты считают, что информация пропагандистского характера может негативно сказываться на молодёжи.

Вопрос: *«Как Вы относитесь к использованию нелицензионного программного обеспечения?»* позволяет понять, какую роль информационная безопасность занимает в жизни респондента:

Петренко А.А.: «Отношусь нейтрально, да, это незаконно, но в данный момент я не могу позволить себе лицензионное ПО, поэтому, например, использую продление «пробного месячного периода» для антивируса, при этом, операционная система у меня всё же лицензионная. Будь у меня большой доход, я бы точно приобретала полностью лицензионное ПО»;

Саяпина А.Ю.: «Нормально отношусь, но считаю, что из- за отсутствия лицензии и появляются многие проблемы, потери личных данных и прочее, от чего могла бы «защитить» лицензионная версия»;

Петров А.О.: «Негативно, я за честное и справедливое пользование»;

Романова А.А.: «Я отношусь нормально, платить за каждый вид услуг среднестатистическому человеку очень проблемно, поэтому необходимо выкручиваться»;

Чеснокова И.В.: «Отношусь нейтрально, не могу выразить определенно положительно или отрицательно»;

Ильин Н.А.: «Нейтрально, иногда это необходимость»;

Шелепин В.И.: «Если это нелицензионное ПО используется частным лицом в личных некоммерческих целях, или коммерческих, но с очень маленьким доходом, то это позволительно. Если оно используется крупной

кампанией, то это уже явное нарушение закона, которое точно требует вмешательства, в отличие от первого случая. Так же вмешательства требует ситуация, если отдельная личность использует нелицензионное ПО для получения больших доходов»;

Зидыганова Е.А.: «Положительно, говорю, как простой бедный студент. Откуда нам на учебу в университете брать столько денег, чтобы содержать лицензионное ПО на компьютере, антивирусы и тому подобное»;

Орлова А.Д.: «Сейчас большинство пользуется нелицензированными программами, это необходимость»;

Антюшин А.В.: «Я отношусь и хорошо и плохо, я понимаю людей которые не могут себе это позволить и понимаю людей которые создавали данный лицензионный продукт, просто они создали и не получат за него никакой выгоды».

На вопрос: *«Какое значение для Вас имеет сохранность Вашей личной информации?»* респонденты ответили:

Петренко А.А.: «Мне очень важно сохранить свои данные и информацию о себе в безопасности, я использую многоуровневые методы защиты»;

Саяпина А.Ю.: «Сохранность моей личной информации имеет для меня огромное значение. Для этого я стараюсь по возможности эти данные защитить»;

Петров А.О.: «Большое значение, информация в современном обществе – все»;

Романова А.А.: «Конечно, сохранность моей личной информации играет для меня высокую и значимую роль»;

Чеснокова И.В.: «Мне важно, чтобы моими личными данными, распоряжалась только я»;

Ильин Н.А.: «Ключевое»;

Шелепин В.И.: «Одно из самых важных, ведь от того, что думают обо мне другие, зависит часть моей жизни».

Зидыганова Е.А.: «Моя личная информация имеет значимую роль в моей жизнедеятельности»;

Орлова А.Д.: «Конечно, достаточно значимое»;

Антюшин А.В.: «Высокое значение».

В результате абсолютно все респонденты отметили высокую значимость сохранности информации в их жизни.

На последний вопрос: *«Как Вы считаете, от кого в первую очередь зависит информационная безопасность человека?»* респонденты ответили:

Петренко А.А.: «От его собственного ответственного отношения к хранению своих данных и обеспечением им безопасность»;

Саяпина А.Ю.: «Считаю, что в большей степени информационная безопасность человека зависит от него самого. Но немалую роль играет и государство, которое должно ограничиваться население от вредоносной информации»;

Петров А.О.: «От самого человека, кто как ни он сам будет распространять информацию»;

Романова А.А.: «Конечно, от самого человека. Сейчас можно рассчитывать и полагаться только на себя»;

Чеснокова И.В.: «Я считаю, что это не зависит ни от кого. Мошенники и взломщики свою жертву определяют случайно и ей может стать любой»;

Ильин Н.А.: «От него самого»;

Шелепин В.И.: «В основном от самого человека. Во- первых, от его знаний в этой информационной безопасности, а во- вторых от того, насколько ценная у него информация».

Зидыганова Е.А.: «От собственной деятельности человека, во многом как он поступит, то и получит»;

Орлова А.Д.: «От самого себя»;

Антюшин А.В.: «От самого человека и от государства».

Подводя итог, необходимо отметить высокую значимость сохранности информации в жизни всех респондентов, независимо от их

профессиональных навыков и профилей обучения. Вопросы, которые касались столкновений с различными информационными угрозами и использованием средств защиты своих данных в Интернете также не выявили существенных различий между студентами- гуманитариями и студентами- программистами. В основном мнения разделились в вопросах, связанных с отношением респондентов к таким действиям правительства, как блокировке торрент- трекеров и возможностью специальных служб собирать, хранить и просматривать переписку или любые личные данные, в качестве способа обеспечения общественной безопасности: студенты- программисты высказывали своё нейтральное отношение, в то время, как студенты- гуманитарии относятся к этому отрицательно. В результате интервью выяснилось, что все респонденты уделяют большое внимание обеспечению своей информационной безопасности: используют антивирусы, различные программы по блокировке рекламы, используют сложные пароли к различным Интернет- сервисам, стараются критически относиться к информации, распространённой в Интернете.

Заключение

Стремительное развитие информатизации в Российской Федерации и проникновение её во все сферы жизненно важных интересов личности, общества и государства повлекли помимо несомненных преимуществ также и появление ряда существенных проблем. Одной из них стала необходимость защиты информации.

Информационная сфера Российской Федерации является важнейшей составляющей жизнедеятельности общества и государства. Вследствие этого обеспечение безопасности национальных интересов Российской Федерации в этой сфере способствует укреплению национальной безопасности Российской Федерации. Информационная сфера играет ключевую роль в реализации многих конституционных прав и свобод граждан, в обеспечении возможности самореализации личности, духовном обновлении, политической и социальной стабильности общества, обеспечении функционирования государства. Она также становится всё более важным фактором развития экономики промышленно развитых стран мира, мировой экономики в целом, а также развития мирового сообщества.

Нормальная жизнедеятельность человеческого общества во всё большей степени зависит от состояния информационной сферы, которая, в связи с этим, всё активней используется для оказания давления на государственную политику разных стран, как со стороны иностранных государств, так и со стороны организованной преступности, международных и национальных террористических группировок.

Таким образом, информационная безопасность становится ключевым фактором обеспечения стабильного развития общества. Поскольку молодёжь является одним из главных механизмов развития общества, обеспечение её информационной безопасности, развития её информационной культуры и подготовка соответствующим образом информированных специалистов

представляется одной из важнейших задач молодёжной политики любой страны.

В результате проведённого исследования удалось выяснить, что молодёжь на сегодняшний день часто сталкиваться с различными угрозами информационной безопасности. В большей степени угрозам подвержены молодые люди школьного возраста. Как выяснилось, школьники менее склонны критически оценивать информацию, полученную в сети Интернет, а также обладают недостаточными знаниями в области обеспечения своей информационной безопасности. Следовательно, возрастает необходимость формирования навыков обеспечения информационной безопасности у современной молодёжи ещё в школьном возрасте. Включение в федеральные образовательные стандарты обучение навыкам первичной информационной безопасности, по мнению многих политических деятелей, может способствовать решению данной проблемы. В частности, вице- спикер Государственной думы Российской Федерации, Ирина Яровая, на заседании Комитета Госдумы по вопросам семьи, женщин и детей заявила: «Действующая образовательная программа, касающаяся пользования Интернетом, упустила самое главное – обучение ребёнка первичным необходимым навыкам личной безопасности в этом информационной пространстве».

В результате интервью со студентами различных специальностей выяснилось, что все респонденты, независимо от профиля обучения, уделяют большое внимание обеспечению своей информационной безопасности, стараются выкладывать меньше личной информации в сеть, а также с недоверием относится к информации, полученной в Интернете. Практически все респонденты, принявшие участие в исследовании, считают, что информационная безопасность человека в первую очередь зависит от него самого.

Список используемой литературы и источников

1. Алексеева, Е.В. Доктрина информационной безопасности Российской Федерации как ключевой аспект правового обеспечения национальной безопасности в информационной сфере / Е.В. Алексеева // Ленинградский юридический журнал. – 2016. – № 4 (46). – С. 97- 103.
2. Алпеев, А.С. Терминология безопасности: кибербезопасность, информационная безопасность / А.С. Алпеев // Вопросы кибербезопасности. – 2014. – № 5 (8). – С. 39- 42.
3. Арутюнян, М.Л. Риски, обусловленные трансформацией социально- политического пространства в современном информационном обществе / М.Л. Арутюнян // Сборники конференций НИЦ Социосфера. – 2014. – № 33. – С. 9.
4. Атаманов, Г.А. Информационная безопасность: сущность и содержание / Г.А. Атаманов // Бизнес и безопасность в России. – 2007. – № 47. – С. 108- 114.
5. Бек, У. Общество риска: На пути к другому модерну / Пер. с нем. В. Седельника, Н. Федоровой. – М.: Прогресс- Традиция, 2000. – 383 с.
6. Белл, Д. Социальные рамки информационного общества // Новая технократическая волна на Западе / Под ред. П.С. Гуревича. – М.: Прогресс, 1986. – 420 с.
7. Белов, А.В. Информационное общество и информационная культура в России: к постановке проблемы / А.В. Белов // Вестн. Волгогр. гос. ун- та. Сер. 7. Философия. – 2009. – № 1 (9). – С. 198- 202.
8. Блусь, П.И. Информатизация общества как фактор повышения качества жизни населения / П.И. Блусь, А.В. Вагина // ARS ADMINISTRANDI. – 2015. – № 3. – С. 5- 18.
9. Богатырева, Ю.И. Модель обеспечения информационной безопасности школьников при создании инфобезопасной среды образовательного

учреждения / Ю.И. Богатырева // Известия ТулГУ. Гуманитарные науки. – 2013. – № 3- 2. – С. 14- 26.

10. Брылева, Е.А. Информационная безопасность несовершеннолетних как часть национальной безопасности / Е.А. Брылева // Вестник Самарского юридического института. – 2014. – № 1 (12). – С. 12- 14.
11. Васильева, М.М. Информационная безопасность России в условиях глобализации / М.М. Васильева // Вестник МГЛУ. – 2010. – № 604. – С. 26- 34.
12. Войскунский, А.Е. Информационная безопасность: психологические аспекты / А.Е. Войскунский // Национальный психологический журнал. – 2010. – № 1. – С. 48- 53.
13. Гидденс, Э. Последствия современности / Э. Гидденс. – М.: Праксис, 2011. – 343 с.
14. Гидденс, Э. Судьба, риск и безопасность / Э. Гидденс / THESIS. – *1994*. – Вып. 5. – С. 40- 102.
15. Дрепа, М.И. Интернет- зависимость как объект научной рефлексии в современной психологии / М.И. Дрепа // Знание. Понимание. Умение. – 2009. – № 2. – С.189- 193.
16. Емельяненко, В.Д. Интернет и ценностно- мировоззренческие основания патриотического воспитания / В.Д. Емельяненко, В.А. Лобач- Граубергер // Новая наука: Теоретический и практический взгляд. – 2016. – № 2- 3 (63). – С. 163- 174.
17. Емельяненко, В.Д. Интернет и ценностно- мировоззренческие основания правосознания / В.Д. Емельяненко, А.М. Богданова, Ю.А. Гнаева //Альманах современной науки и образования. – 2015. – № 7 (97). – С. 66- 70.
18. Зленко, Н.Н. Философское осмысление современных подходов общественного развития / Н.Н. Зленко // Філософія науки: традиції та інновації. – 2011. – № 2 (4). – С. 50- 62.

19. Илюшин, С.Н. Общество и социальные риски: современное состояние и сценарии будущего / С.Н. Илюшин // Научные и образовательные проблемы гражданской защиты. – 2013. – № 1. – С. 98- 101.
20. Ищенко, М.В. Информационное общество: подходы к определению сущности категорий / М.В. Ищенко // Вестник ОмГУ. Серия: Экономика. – 2007. – № 1 – С. 47- 54.
21. Кастельс, М. Информационная эпоха: экономика, общество и культура / Пер. с англ. под науч. ред. О. И. Шкаратана. – М.: ГУ ВШЭ, 2000. – 608 с.
22. Клементьев, А.С. Противодействие кибертерроризму и киберэкстремизму: новая сфера правоохранительной деятельности / А.С. Клементьев // Противодействие терроризму. Проблемы XXI века. № 2 – М.: ЗАО «Изд- во «Современная экономика и право». – 2013. – С. 25- 30.
23. Колин, К.К. Гуманитарные проблемы формирования информационного общества / К.К. Колин // Вестн. Кемеров. гос. ун- та культуры и искусств. – Кемерово, 2010. – № 12. – С. 8- 19.
24. Костина, А.В. Культура информационного общества: тенденции и противоречия развития / А.В. Костина // Вестник Рязанского государственного университета им. С.А. Есенина. – 2009. – № 24. – С. 72- 98.
25. Крапивенский, А.С. Подготовка специалистов в сфере информационной безопасности: необходимость гуманитарной эволюции / А.С. Крапивенский // Вестник ВолГУ. Серия 7: Философия. Социология и социальные технологии. – 2008. – № 2. – С. 197.
26. Крапивенский, А.С. Социологический и социально- психологический подходы к определению концепта «информационная безопасность» в рекламной коммуникации / А.С. Крапивенский // Научный вестник Волгоградской академии государственной службы. Серия: Политология и социология. – 2010. – № 2. – С. 53.

27. Крюкова, Е.Н. Интернет- зависимость как один из показателей нарушения межличностных отношений / Е.Н. Крюкова // Вестник Самарского государственного технического университета. Серия: Психолого- педагогические науки. – 2012. – № 1. – С. 87- 92.
28. Курносов, И.Н. Роль государства в формировании информационного общества в России / И.Н. Курносов // Вестник РФФИ. – 1999. – № 3. – С. 15.
29. Логинова, С.А. Проблемы современного информационного общества / С.А. Логинова // Изв. ВГПУ. – 2014. – № 1 (262). – С. 20- 22.
30. Лопатин, В.Н. Информационная безопасность России: Человек, общество, государство. Серия: Безопасность человека и общества / В.Н. Лопатин. – М.: 2000. – 428 с.
31. Лопатина, Н.В. Информационные специалисты: социология управления / Н.В. Лопатина – М.: Академический Проект, 2006. – 203 с.
32. Луман, Н. Понятие риска / Н. Луман // THESIS. – *1994*. – Вып. 5. – С. 4- 160.
33. Лызь, Н.А. Информационно- психологическая безопасность в системах безопасности человека и информационной безопасности государства / Н.А. Лызь, Г.Е. Веселов, А.Е. Лызь // Известия ЮФУ. Технические науки. 2014. – Т. 157. – № 8. – С. 58- 66.
34. Мардеева, Д.С. Профилактика киберэкстремизма на основе формирования ценностей молодёжи / Д.С. Мардеева // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодёжи. Материалы внутривузовской конференции. Под ред. Г.Н. Чусавитиной, Е.В. Черновой, О.Л. Колобовой. 2015. Магнитогорск: Магнитогорский государственный технический университет им. Г.И. Носова. – 2015. – С. 283- 289.

35. Марков, А.А. Понятие и характеристика информационных рисков, опасностей и угроз в современном постиндустриальном обществе / А.А. Марков // Вестник Волгоградского государственного университета. Серия 7: Философия. Социология и социальные технологии. – 2010. – № 1. – С. 125.
36. Маслакова, Е.А. Информационная безопасность: концептуальные основы защиты информации / Е.А. Маслакова // Наука и практика. – 2014. – № 2 (59). – С. 93- 96.
37. Матюх, Е.Т. Теории «общества риска» в современной гуманитарной науке / Е.Т. Матюх // Теория и практика общественного развития. – 2012. – № 7. – С. 33- 36.
38. Морозова, А.А. Медиа- безопасность в эпоху информации / А.А. Морозова // Информационное поле современной России: практики и эффекты: Материалы IX Международной научно- практической конференции, 18- 20 октября 2012 г. / под ред. Р.П. Баканова: в 2- х т. – Т. 1. – Казань: Казан. ун- т, 2012. – С. 280- 287.
39. Пархоменко, Н.Г. Выявление угроз информационной безопасности в реальном времени, комплексы контроля информационной безопасности / Н.Г. Пархоменко, Б.М. Боташев, П.М. Колобанов, Е.С. Григоренко // Известия ЮФУ. Технические науки. – 2003. – № 4. – С. 325- 326.
40. Петров, В.П., Информационная безопасность человека и общества: учебное пособие / В.П. Петров, С.В. Петров. – М.: Изд- во НЦ ЭНАС, 2007. – 336 с.
41. Пищулина, Т.В. Специалист в условиях информационного общества / Т.В. Пищулина // Человек. Спорт. Медицина. – 2008. – № 13 (113). – С. 67- 71.
42. Потехина, И.П. Развитие информационно- коммуникационных технологий в условиях глобализации / И.П. Потехина // Вестник

Саратовского государственного социально- экономического университета. – 2012. – № 2. – С. 36- 40.

43. Ракитов, А.И. Информация, наука, технология в глобальных исторических изменениях / А.И. Ракитов – М.: РАН. Институт научной информации, 1998. – 104 с.
44. Руденко, О.Ю. Киберэкстремизм в молодёжной среде / О.Ю. Руденко // Сборники конференций НИЦ Социосфера. – 2013. – № 55. – С. 33- 35.
45. Сладкова, О.Б. Использование информационного мониторинга для манипуляции общественным сознанием/ О.Б. Сладкова // Вестник МГУКИ. – 2005. – Вып. 2. – С. 127.
46. Старкова, Н.А. Социальные проблемы распространения киберэкстремизма в молодёжной среде / Н.А. Старкова // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодёжи. Материалы внутривузовской конференции. Под редакцией Г.Н. Чусавитиной, Е.В. Черновой, О.Л. Колобовой. 2015. – Магнитогорск: Магнитогорский государственный технический университет им. Г.И. Носова. – 2015. – С. 419- 427.
47. Степанищенко, О.В. Исследование молодежи как особой социальной группы в социально- гуманитарных науках / О.В. Степанищенко // Научный журнал КубГАУ– ScientificJournalofKubSAU. – 2011. – № 73. – С. 587- 600.
48. Уэбстер, Ф. Теории информационного общества / Ф. Уэбстер. – М.: Аспект Пресс, 2004. – 400 с.
49. Федорова, Ж.В. Информационная безопасность и цензура в современной России: о соотношении понятий / Ж.В. Федорова // Путь науки. – 2014. – № 5 (5). – С. 75- 77.
50. Чеботарева, А.А. Информационное право: учеб. пособие / А.А. Чеботарева – М.: Юридический институт МИИТа, 2014. – 162 с.

51. Чурашева, О.Л. Информационная культура и информационная безопасность личности / О.Л. Чурашева // Теория и практика общественного развития. – 2014. – № 16. – С. 188- 190.
52. Шарин, В.И. Социальные риски как угрозы социальному положению и защита от них / В.И. Шарин // Известия УрГЭУ. – 2013. – № 6 (50). – С. 118- 124.
53. Юсупов, Р.М. Информационная безопасность, кибербезопасность и смежные понятия: CyberSecurity VS Информационной безопасности / Р.М. Юсупов, В.М. Шишкин // Информационное противодействие угрозам терроризма. – № 21 (21). – 2013. – С. 27- 35.
54. Доктрина информационной безопасности Российской Федерации: указ Президента Российской Федерации от 05.12.2018 г. № 646. [Электронный ресурс]. – Режим доступа: URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 03.02.2019).

Приложение 1

Программа исследования

Эмпирическое исследование:

«Представление об информационной безопасности различных групп молодежи города Тольятти»

МЕТОДОЛОГИЧЕСКИЙ РАЗДЕЛ

Обоснование проблемы исследования. В условиях информатизации общества информационное воздействие на личность приобретает глобальные масштабы. Опасность для человека в информационном обществе, в первую очередь, связана с тем, что развитие глобальных сетей, телевидения, компьютерных коммуникаций и других информационных систем создают широкие возможности для воздействия на общественное сознание и манипуляции этим сознанием[42].

Информационные технологии оказывают значительное влияние на ценностные установки и поведенческие ориентиры людей, определяя их деятельность. Наиболее уязвима в этом отношении молодёжь, находящаяся в процессе личностного формирования[43].

К факторам информационно-образовательной среды, которые могут стать опасностями информационной безопасности современной молодёжи, исследователи данного вопроса относят следующие:

- доступность и неограниченный объем поступающей информации;
- наличие в информационной среде средств манипуляции сознанием, воздействующих на психические и физиологические системы человека;

[42] Логинова С.А. Проблемы современного информационного общества // Изв. ВГПУ. – 2014. – № 1 (262). – С. 20- 22.
[43] См.: Маслакова Е.А. Информационная безопасность: концептуальные основы защиты информации // Наука и практика. – 2014. – № 2 (59). – С. 93- 96.

- наличие в информационном контенте специфических элементов, целенаправленно изменяющих психофизиологическое состояние детей и подростков[44].

Главной угрозой в информационной среде, на сегодняшний день, является киберэкстремизм – это криминальное использование технологий приёма, обработки, передачи, хранения и распространения информационных сообщений экстремистского характера. Молодёжь – основная аудитория, которая подвержена киберэкстремизму[45]. Перед экстремистами в информационной среде открываются широкие возможности информационно- коммуникативных технологий: пропаганда своих взглядов по средствам сети Интернет, подготовка террористов, вербовка единомышленников, сбор информации о предполагаемых целях и объектах шантажа, сбор пожертвований, создание и регистрация информационных ресурсов[46]. В этой связи большое значение имеет процесс формирования особых представлений об информационной безопасности и способности противостоять информационным угрозам в современном обществе.

Подросток анализирует и оценивает полученную информацию в соответствии со сформированными у него родителями, образовательными учреждениями, обществом и государством способностями к оцениванию угроз в информационном пространстве, умениями информационной самозащиты, а также особенностями его личностной информационной среды[47]. В современных социально-экономических условиях наблюдается всё большая вовлеченность молодёжи в информационную сферу. Как социально-возрастная группа молодёжь обладает рядом особенностей. Во-первых, ей присуще неполное включение в социально-экономические отношения. Во-

[44] Богатырева Ю.И. Модель обеспечения информационной безопасности школьников при создании инфобезопасной среды образовательного учреждения // Известия ТулГУ. Гуманитарные науки. – 2013. – № 3- 2. – С. 21.
[45] Мардеева Д.С. Профилактика киберэкстремизма на основе формирования ценностей молодёжи // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодёжи. Материалы внутривузовской конференции. Под ред. Г.Н. Чусавитиной, Е.В. Черновой, О.Л. Колобовой. 2015. Магнитогорск: Магнитогорский государственный технический университет им. Г.И. Носова. – 2015. – С. 283- 289.
[46] Руденко О.Ю. Киберэкстремизм в молодёжной среде // Сборники конференций НИЦ Социосфера. – 2013. – № 55. – С. 33- 35.
[47] Богатырева Ю.И. Модель обеспечения информационной безопасности школьников при создании инфобезопасной среды образовательного учреждения // Известия ТулГУ. Гуманитарные науки. – 2013. – № 3- 2. – С. 14- 26.

вторых, одновременно именно она в наибольшей степени мобильна, инициативна. По сути, от качества её потенциала зависят перспективы развития экономики, разработка и внедрение инноваций в сферах науки, культуры, производства, новых социальных стратегий.

Таким образом, на сегодняшний день является важным, чтобы подрастающее поколение имело чёткие представления об источниках и факторах, обусловливающих возникновение социальных конфликтов в информационной сфере, основных механизмах их регулирования, а также учитывало угрозы негативных информационных воздействий на индивидуальное и общественное сознание, психику людей и их здоровье[48].

Целью данного социологического исследования является сравнение представлений об информационной безопасности различных групп молодёжи.

В соответствии с целью были поставлены следующие **задачи**:

1. определить цели использования сети Интернет молодёжью;

2. определить отношение молодёжи к основным информационным угрозам;

3. проанализировать, с какими нарушениями информационной безопасности сталкивается молодёжь;

4. сравнить отношение различных групп молодёжи к проблеме информационной безопасности;

5. определить отношение молодёжи к основным мерам обеспечения информационной безопасности.

Объектом аналитического исследования является молодёжь, дифференцированная по возрасту на две равные группы респондентов. Первая группа включает школьников в возрасте 14- 18 лет, респонденты второй группы – студенты в возрасте 19- 24 лет.

---

[48] Чурашева О.Л. Информационная культура и информационная безопасность личности // Теория и практика общественного развития. – 2014. – № 16. – С. 188- 190.

Предмет исследования состоит в изучении представлений об информационной безопасности двух групп молодёжи: первая группа – 14-18 лет, вторая группа – 19-24 лет.

Гипотезы исследования:

1. Предположительно, студенты более информированы о средствах обеспечения информационной безопасности, чем школьники;

2. Школьники чаще, чем студенты сталкиваются с угрозами информационной безопасности в Интернете;

3. Предположительно, студенты более заинтересованы в обеспечении своей информационной безопасности;

4. Большинство респондентов склонно положительно оценивать эффективность мер обеспечения государством информационной безопасности молодёжи;

5. Наиболее эффективным способом обеспечения информационной безопасности респонденты считают информирование молодёжи о правовых актах, обеспечивающих безопасность в информационной сфере.

Системный анализ объекта исследования

Информационная компетентность респондентов:

- цели использования сети Интернет;
- источники информации при выполнении учебных заданий;
- отношение преподавателей к источникам получения информации при выполнении учебных заданий;

Отношение к информационным угрозам:

- угрозы национальной безопасности, связанные с распространением Интернета;
- негативные социальные последствия распространения Интернета;
- факты информационной угрозы;
- отношение к плагиату;

- отношение к «Интернет-пиратству»;

Обеспечение информационной безопасности:

- использование средств обеспечения информационной безопасности;
- эффективность мер информационной безопасности;
- личная ответственность за обеспечение средств информационной безопасности;
- необходимость знаний для обеспечения информационной безопасности;
- информированность о мерах обеспечения государством информационной безопасности;
- оценка эффективности государственной политики по обеспечению безопасности;

Социально-демографические характеристики:

- пол (опрашиваются мужчины и женщины в любой пропорции);
- возраст (14-18 лет / 19-24 лет);
- материальное положение.

Теоретическая интерпретация социологических понятий

В данном исследовании мы руководствовались следующими понятиями и категориями:

Информационная безопасность – состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере; процесс обеспечения конфиденциальности, целостности и доступности информации.

Информационная угроза – совокупность условий и факторов, создающих опасность нарушения информационной безопасности. Под угрозой (в общем) понимается потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам.

Интернет-ресурс (синонимы «веб- ресурс, веб-сайт, веб-сервис, сайт») – это совокупность интегрированных средств технического и программно-аппаратного характера, а также информации, предназначенной для публикации во Всемирной паутине. Интернет-ресурс может содержать информацию в текстовой, графической и мультимедийной форме.

Политика государства по обеспечению информационной безопасности – совокупность стратегических и текущих задач внутренней и внешней политики государства по обеспечению информационной безопасности.

Киберэкстремизм – это новая форма экстремизма, которая осуществляется через глобальную сеть Интернет; это криминальное использование технологий приема, обработки, передачи, хранения и распространения информационных сообщений экстремистского характера.

Нарушение авторского права (также контрафакция, от лат. contrafactio – подделка; или – в случае имущественных АП – «пиратство») – это правонарушение, суть которого составляет использование произведений науки, литературы и искусства, охраняемых авторским правом, без разрешения авторов или правообладателей, или с нарушением условий договора о использовании таких произведений.

Операционализация социологических понятий

Данное исследование предполагает выяснение в первом блоке вопросов состояния информационной компетентности респондентов. Для начала узнаем, *как чаще всего респонденты используют Интернет:*

- ✓ Общаюсь в социальных сетях
- ✓ Играю в сетевые игры
- ✓ Нахожу нужную информацию
- ✓ Скачиваю материалы (книги, рефераты, фильмы…)
- ✓ Пользуюсь электронной почтой
- ✓ Оплачиваю различные услуги, делаю покупки

- ✓ Другое_____

Номинальная шкала позволит нам выяснить, *какие* именно *источники из Интернета* используют на сегодняшний день респонденты при выполнении учебных заданий:

- ✓ Электронными библиотеками ВУЗов
- ✓ Сайтами научных журналов
- ✓ Бесплатными электронными библиотеками
- ✓ Платными электронными библиотеками
- ✓ Сайтами, на которых можно заказать работу
- ✓ Бесплатными сайтами с готовыми работами
- ✓ Не пользуюсь Интернет источниками

Также будет интересно узнать, *как преподаватели относятся к тому, что при выполнении учебных заданий,* респонденты *используют материалы из Интернета:*

- Разрешают пользоваться любыми материалами из Интернета
- Требуют анализа, обдуманного отношения к материалам из Интернета
- Запрещают пользоваться материалами из Интернета
- Другое _____

С помощью следующего блока вопросов мы попытаемся проанализировать отношение респондентов к современным информационным угрозам. Для начала узнаем, *какие угрозы, по мнению респондентов, наносят ущерб национальной безопасности:*

- ✓ Провоцирование межэтнической и межконфессиональной напряженности
- ✓ Пропаганда эгоистических установок и потребительского образа жизни снижение значимости семейных ценностей
- ✓ Пропаганда сексуальной «распущенности»
- ✓ Вовлечение молодежи в асоциальные субкультуры
- ✓ Размывание традиционной системы ценностей

- ✓ Распространение экстремистских взглядов
- ✓ Пропаганда национального превосходства и исключительности
- ✓ Пропаганда насилия и жестокости
- ✓ Рост нарко- и алкогольной зависимости среди молодежи
- ✓ Мошенничество, вовлечение в деятельность финансовых пирамид
- ✓ Вовлечение в тоталитарные, религиозных секты
- ✓ Формирование зависимости от азартных игр

Далее выясним, *какие негативные социальные последствия для молодёжи имеет распространение Интернета:*

- ✓ Малоподвижный образ жизни
- ✓ Обезличенное, анонимное общение
- ✓ Снижение уровня культуры
- ✓ Негативные эмоциональные состояния
- ✓ Снижение уровня интеллекта
- ✓ Игромания, киберзависимость
- ✓ Проблемы, связанные с сексуальным поведением
- ✓ Формирование поведения, связанного с риском для жизни
- ✓ Пропаганда вредных привычек (наркомании, курения и т.д.)
- ✓ Социальная пассивность, инфантильность

С помощью следующего вопроса, мы поймём, с *какими нарушениями информационной безопасности сталкивались респонденты:*

- ✓ Хищение средств с платёжной карты
- ✓ Распространение спама
- ✓ Вирусные атаки
- ✓ Хищение персональных данных
- ✓ Мошенничество с использованием электронных устройств
- ✓ Нарушение авторских прав (плагиат)
- ✓ Информационное «пиратство» незаконное распространение книг, фильмов

- ✓ Хищение логина и пароля (для социальных сетей, электронной почты)
- ✓ Не сталкивался(лась)
- ✓ Другое (укажите, что именно) ____

Следующий вопрос позволит нам выяснить, *с какими явлениями информационного воздействия сталкивались респонденты:*

- o Оскорбления, употребление нецензурных слов, выражений
- o Фото и видео порнографического содержания
- o Информационное насилие, жестокие видеосюжеты, запугивающие, угрожающие кадры
- o Навязчивые предложения знакомств в Интернете, в социальных сетях, «письма счастья» и т.п.
- o Угрозы физического наказания
- o Шантаж, принуждение к чему-либо
- o Побуждение к курению, употреблению алкоголя, жестоким или опасным действиям

Далее, с помощью порядковой шкалы, выясним, *как респонденты относятся к такому явлению как «Интернет-пиратство»:*

- Положительно, это позволяет получить бесплатный доступ к играм, книгам, фильмам, музыке
- Скорее, положительно. Это вынужденное средство. Лицензионный доступ стоит дорого
- Скорее, отрицательно это нарушает права тех, кто владеет лицензией
- Отрицательно. Это нарушение закона.

Следующий блок вопросов направлен на то, чтобы определить отношение респондентов к обеспечению информационной безопасности молодёжи. Для начала следует узнать, *какими средствами обеспечения информационной безопасности пользуются* респонденты:

- ✓ Антивирусные программы
- ✓ Антиспамовые фильтры

- ✓ Средства идентификации и электронные ключи
- ✓ Межсетевые экраны
- ✓ Средства авторизации
- ✓ Другое_____

Также будет полезно выяснить, *кто,* по мнению респондентов, *должен обеспечивать информационную безопасность молодёжи*:

- Да, каждый человек должен заботиться о своей информационной безопасности
- Нет, этим должны заниматься специальные государственные службы
- Затрудняюсь ответить

Ранговая шкала позволит нам выяснить, *как по 5- балльной системе (5 – высокая эффективность, 1 – низкая эффективность, 0 – затрудняюсь ответить*) респонденты определяют *эффективность следующих мер обеспечения информационной безопасности:*

- o Информирование молодежи о правовых актах, обеспечивающих безопасность в информационной сфере
- o Работа государственных и правоохранительных органов по профилактике преступлений в информационной среде
- o Раскрытие преступлений, связанных с использованием информационных технологий
- o Ограничение доступа молодежи к информационным ресурсам, представляющим опасность
- o Формирование информационной и коммуникативной компетентности молодежи

Далее следует выяснить, насколько респонденты информированы о следующих средствах обеспечения государством информационной безопасности:

- o Государственный контроль (контроль почтовых отправлений, телеграфных и иных сообщений, прослушивание телефонных

переговоров при осуществлении оперативно-розыскных мероприятий)

- Запрет на пропаганду террористической деятельности
- Защита персональных данных
- Защита права на собственное изображение
- Разработка нормативно-правовых актов по обеспечению информационной безопасности

Затем мы выясним, *какие знания*, по мнению респондентов, *могут способствовать повышению информационной безопасности:*

- ✓ О правах личности
- ✓ О способах защиты прав личности
- ✓ О наказаниях за преступления в информационной сфере
- ✓ О факторах, угрожающих жизни, здоровью
- ✓ О криминальной ситуации
- ✓ О защите от информации, представляющей опасность для жизни, здоровья

Дать *оценку эффективности мер, предпринимаемых государством для обеспечения информационной безопасности*, нам позволит определить порядковая шкала:

- Эффективные
- Недостаточно эффективные
- Неэффективные
- Затрудняюсь оценить

Завершит анкету блок вопросов, отражающих социально-демографические характеристики респондентов.

С помощью номинальной шкалы выясним *пол* респондентов:

- Мужской
- женский

С помощью интервальной шкалы, выясним, к какой возрастной группе принадлежит респондент:

- 14-18 лет
- 19-24 лет

И в завершение мы поинтересуемся, как респонденты оценивают своё материальное положение:

- Выше среднего (чаще всего не имеем материальных затруднений)
- Среднее (иногда испытываем материальные трудности)
- Ниже среднего (приходится на многом экономить)

Приложение 2

Анкета исследования

Уважаемый респондент!

Кафедра «Социология» Тольяттинского государственного университета проводит социологическое исследование с целью сравнения представлений об информационной безопасности молодёжи. Просим Вас ответить на все вопросы анкеты, выбрав вариант ответа, более точно отражающий Ваше мнение. Некоторые вопросы предполагают несколько вариантов ответа. Ваши ответы будут использоваться только в обобщенном виде.

Заранее благодарим Вас за участие в социологическом исследовании!

1. **Как Вы чаще всего используете Интернет? (***можно отметить* ***несколько*** *вариантов ответа)*

1. Общаюсь в социальных сетях
2. Играю в сетевые игры
3. Нахожу нужную информацию
4. Скачиваю материалы (книги, рефераты, фильмы…)
5. Пользуюсь электронной почтой
6. Оплачиваю различные услуги, делаю покупки
7. Другое_____

2. **Какими источниками из Интернета Вы пользуетесь при выполнении учебных заданий?**

1. Электронными библиотеками ВУЗов
2. Сайтами научных журналов
3. Бесплатными электронными библиотеками
4. Платными электронными библиотеками
5. Сайтами, на которых можно заказать работу
6. Бесплатными сайтами с готовыми работами
7. Не пользуюсь Интернет источниками
8. Другое_____

3. **Как Ваши преподаватели относятся к тому, что, выполняя задание, ученики (студенты) используют материалы из Интернета? (***выберите, пожалуйста,* ***только один*** *вариант ответа)*

1. Разрешают пользоваться любыми материалами из Интернета
2. Требуют анализа, обдуманного отношения к материалам из Интернета
3. Запрещают пользоваться материалами из Интернета
4. Другое _____

4. **Какие угрозы, существующие в информационном пространстве, по Вашему мнению, наносят ущерб национальной безопасности?** *(выберите столько вариантов ответов, сколько считаете нужным)*

1. Провоцирование межэтнической и межконфессиональной напряженности
2. Пропаганда эгоистических установок и потребительского образа жизни снижение значимости семейных ценностей
3. Пропаганда сексуальной «распущенности»
4. Вовлечение молодежи в асоциальные субкультуры

5. Размывание традиционной системы ценностей
6. Распространение экстремистских взглядов
7. Пропаганда национального превосходства и исключительности
8. Пропаганда насилия и жестокости
9. Рост нарко- и алкогольной зависимости среди молодежи
10. Мошенничество, вовлечение в деятельность финансовых пирамид
11. Вовлечение в тоталитарные, религиозных секты
12. Формирование зависимости от азартных игр
13. Другое_____

5. Какие негативные социальные последствия для молодёжи имеет распространение Интернета? *(выберите столько вариантов ответа, сколько считаете нужным)*

1. Малоподвижный образ жизни
2. Обезличенное, анонимное общение
3. Снижение уровня культуры
4. Негативные эмоциональные состояния
5. Снижение уровня интеллекта
6. Игромания, киберзависимость
7. Проблемы, связанные с сексуальным поведением
8. Формирование поведения, связанного с риском для жизни
9. Пропаганда вредных привычек (наркомании, курения и т.д.)
10. Социальная пассивность, инфантильность
11. Другое_____

6. Сталкивались ли Вы со следующими нарушениями информационной безопасности: *(выберите столько вариантов ответа, сколько считаете нужным)*

1. Хищение средств с платёжной карты
2. Распространение спама
3. Вирусные атаки
4. Хищение персональных данных
5. Мошенничество с использованием электронных устройств
6. Нарушение авторских прав (плагиат)
7. Информационное «пиратство» незаконное распространение книг, фильмов
8. Хищение логина и пароля (для социальных сетей, электронной почты)
9.Не сталкивался(лась)
10. Другое (укажите, что именно) _____

7. При использовании Интернета сталкивались ли Вы со следующими явлениями… *(отметьте **один** вариант ответа в каждой строке)*

	Да	**Нет**
1. Оскорбления, употребление нецензурных слов, выражений	1	2
2. Фото и видео порнографического содержания	1	2
3. Информационное насилие, жестокие видеосюжеты, запугивающие, угрожающие кадры	1	2
4. Навязчивые предложения знакомств в Интернете, в социальных сетях, «письма счастья» и т.п.	1	2
5. Угрозы физического наказания	1	2
6. Шантаж, принуждение к чему-либо	1	2
7. Побуждение к курению, употреблению алкоголя, жестоким или	1	2

опасным действиям		

8. Как Вы относитесь к «Интернет-пиратству»? *(отметьте, пожалуйста, только **один** вариант ответа)*

1. Положительно, это позволяет получить бесплатный доступ к играм, книгам, фильмам, музыке.
2. Скорее, положительно. Это вынужденное средство. Лицензионный доступ стоит дорого.
3. Скорее, отрицательно это нарушает права тех, кто владеет лицензией.
4. Отрицательно. Это нарушение закона.

9. Какими средствами обеспечения информационной безопасности Вы пользуетесь? *(выберите столько вариантов ответа, сколько считаете нужным)*

1. Антивирусные программы
2. Антиспамовые фильтры
3. Средства идентификации и электронные ключи
4. Межсетевые экраны
5. Средства авторизации
6. Другое_____

10. Как Вы считаете, должны ли Вы заниматься обеспечением своей информационной безопасности? *(отметьте, пожалуйста, **один** вариант ответа)*

1. Да, каждый человек должен заботиться о своей информационной безопасности
2. Нет, этим должны заниматься специальные государственные службы
3. Затрудняюсь ответить

11. Какова, по Вашему мнению, эффективность следующих мер обеспечения информационной безопасности? (*оцените, пожалуйста, по 5- балльной системе, 5 – высокая эффективность, 1 – низкая эффективность, 0 – затрудняюсь ответить)*

Информирование молодёжи о правовых актах, обеспечивающих безопасность в информационной сфере	_____(баллов)
Работа государственных и правоохранительных органов по профилактике преступлений в информационной среде	_____(баллов)
Раскрытие преступлений, связанных с использованием информационных технологий	_____(баллов)
Ограничение доступа молодёжи к информационным ресурсам, представляющим опасность	_____(баллов)
Формирование информационной и коммуникативной компетентности молодёжи	_____(баллов)

12. Насколько Вы информированы о средствах обеспечения государством информационной безопасности? (*отметьте, пожалуйста, ответ в каждой строке)*

	Информирован хорошо	Информирован недостаточно	Не информирован
1. Государственный контроль (контроль почтовых отправлений,	3	2	1

телеграфных и иных сообщений, прослушивание телефонных переговоров при осуществлении оперативно-розыскных мероприятий)			
2. Запрет на пропаганду террористической деятельности	3	2	1
3. Защита персональных данных	3	2	1
4. Защита права на собственное изображение	3	2	1
5. Разработка нормативно-правовых актов по обеспечению информационной безопасности	3	2	1

13. Какие знания, по Вашему мнению, могут способствовать повышению информационной безопасности? *(выберите, пожалуйста, не более 3- х вариантов ответа)*

1. О правах личности
2. О способах защиты прав личности
3. О наказаниях за преступления в информационной сфере
4. О факторах, угрожающих жизни, здоровью
5. О криминальной ситуации
6. О защите от информации, представляющей опасность для жизни, здоровья
7. Другое_____

14. Как Вы оцениваете меры, предпринимаемые государством для обеспечения информационной безопасности? *(отметьте, пожалуйста,* ***один*** *вариант ответа)*

1. Эффективные
2. Недостаточно эффективные
3. Неэффективные
4. Затрудняюсь оценить

15. Укажите, пожалуйста, Ваш пол:

1. Мужской
2. Женский

16. Укажите, пожалуйста, Ваш возраст:

1. 14- 18 лет
2. 19- 24 лет

17. Как Вы оцениваете материальное положение Вашей семьи? *(отметьте, пожалуйста,* ***только один*** *вариант ответа)*

1. Выше среднего (чаще всего не имеем материальных затруднений)
2. Среднее (иногда испытываем материальные трудности)
3. Ниже среднего (приходится на многом экономить)

Спасибо за участие в исследовании!

Приложение 3

Таблицы распределений по результатам анкетирования

1. Как Вы чаще всего используете Интернет?	Всего абсолютн	Возраст 14-18	Возраст 14-18 в %	Возраст 19-24 абсолют	Возраст 19-24 в %
1.Общаюсь в социальных сетях	64	28	26	36	26
2. Играю в сетевые игры	24	13	12	11	8
3. Нахожу нужную информацию	51	20	18	31	22
4. Скачиваю материалы (книги, рефераты, фильмы…)	48	22	20	26	18
5. Пользуюсь электронной почтой	42	18	16	24	17
6. Оплачиваю различные услуги, делаю покупки	20	8	8	12	9
7. Другое	0	0	0	0	0
Всего	100	50	100	50	100

2. Какими источниками из Интернета Вы пользуетесь при выполнении учебных заданий?	Всего абсолютн	Возраст 14-18	Возраст 14-18 в %	Возраст 19-24 абсолют	Возраст 19-24 в %
1. Электронными библиотеками ВУЗов	33	7	7	26	23
2. Сайтами научных журналов	30	14	13	16	14
3. Бесплатными электронными библиотеками	51	25	24	26	24
4. Платными электронными библиотеками	23	15	15	8	8
5. Сайтами, на которых можно заказать работу	32	18	17	14	13
6. Бесплатными сайтами с готовыми работами	37	19	18	18	17
7. Не пользуюсь Интернет источниками	7	6	6	1	1
8. Другое	0	0	0	0	
Всего:	100	50	100	50	100

3. Как Ваши преподаватели относятся к тому, что, выполняя задание, ученики (студенты) используют материалы из Интернета?	Всего абсолютн	Возраст 14-18	Возраст 14-18 в %	Возраст 19-24 абсолют	Возраст 19-24 в %
1. Разрешают пользоваться любыми материалами из Интернета	49	28	56	21	42
2. Требуют анализа, обдуманного отношения к материалам из Интернета	32	10	20	22	44
3. Запрещают пользоваться материалами из Интернета	18	12	24	6	12
Другое	1	0	0	1	2
Всего:	100	50	100	50	100

4. Какие угрозы, существующие в информационном пространстве, по Вашему мнению, наносят ущерб национальной безопасности?	Всего абсолютные	Возраст 14-18 абсолют	Возраст 14-18 в %	Возраст 19-24 абсолют	Возраст 19-24 в %
1. Провоцирование межэтнической и межконфессиональной напряженнос	39	21	17	18	10
2. Пропаганда эгоистических установок и потребительского образа жизни снижение значимости семейных ценностей	40	17	13	23	13
3. Пропаганда сексуальной «распущенности»	24	11	9	13	7
4. Вовлечение молодежи в асоциальные субкультуры	27	15	12	12	7
5. Размывание традиционной системы ценностей	22	10	8	12	7
6. Распространение экстремистских взглядов	21	9	7	12	7
7. Пропаганда национального превосходства и исключительности	26	10	8	16	9
8. Пропаганда насилия и жестокости	21	6	5	15	9
9. Рост нарко- и алкогольной зависимости среди молодежи	24	10	8	14	8
10. Мошенничество, вовлечение в деятельность финансовых пирамид	26	7	6	19	11
11. Вовлечение в тоталитарные, религиозных секты	16	5	4	11	6
12. Формирование зависимости от азартных игр	11	3	2	8	5
13. Другое	2	1	1	1	1
Всего:	100	50	100	50	100

5. Какие негативные социальные последствия для молодёжи имеет распространение Интернета?	Всего абсолютные	Возраст 14-18 абсолют	Возраст 14-18 в %	Возраст 19-24 абсолют	Возраст 19-24 в %
1. Малоподвижный образ жизни	37	13	12	24	13
2. Обезличенное, анонимное общение	26	7	6	19	12
3. Снижение уровня культуры	32	15	13	17	11
4. Негативные эмоциональные состояния	31	12	11	19	12
5. Снижение уровня интеллекта	33	18	16	15	9
6. Игромания, киберзависимость	32	13	12	19	12
7. Проблемы, связанные с сексуальным поведением	27	17	15	10	8
8. Формирование поведения, связанного с риском для жизни	13	6	5	7	6
9. Пропаганда вредных привычек (наркомании, курения и т.д.)	24	9	8	15	10
10. Социальная пассивность, инфантильность	11	2	2	9	6
11. Другое	1	0	0	1	1
Всего:	100	50	100	50	100

6. Сталкивались ли Вы со следующими нарушениями информационной безопасности?	Всего абсолютные	Возраст 14-18 абсолют	Возраст 14-18 в %	Возраст 19-24 абсолют	Возраст 19-24 в %
1. Хищение средств с платёжной карты	26	11	10	15	13
2. Распространение спама	29	12	12	17	15
3. Вирусные атаки	32	18	17	14	11
4. Хищение персональных данных	16	9	8	7	6
5. Мошенничество с использованием электронных устройств	21	12	11	9	7
6. Нарушение авторских прав (плагиат)	26	13	12	13	11
7. Информационное «пиратство» незаконное распространение книг, фильм	30	14	13	16	14
8. Хищение логина и пароля (для социальных сетей, электронной почты)	34	15	14	19	16
9.Не сталкивался(лась)	10	3	3	7	6
10.Другое	1	0	0	1	1
Всего:	100	50	100	50	100

7. При использовании Интернета сталкивались ли Вы со следующими явлениями…	Всего абсолютные	Возраст 14-18 абсолют	Возраст 14-18 в %	Возраст 19-24 абсолют	Возраст 19-24 в %
1. Оскорбления, употребление нецензурных слов, выражений					
Да	69	28	56	41	82
Нет	31	22	44	9	18
2. Фото и видео порнографического содержания					
Да	64	28	56	36	72
Нет	36	22	44	14	28
3. Информационное насилие, жестокие видеосюжеты, запугивающие, угрожающие кадры					
Да	58	27	54	31	62
Нет	42	23	46	19	38
4. Навязчивые предложения знакомств в Интернете, в социальных сетях, «письма счастья» и т.п.					
Да	63	28	56	35	70
Нет	37	22	44	15	30
5. Угрозы физического наказания					
Да	32	14	28	18	36
Нет	68	36	72	32	64
6. Шантаж, принуждение к чему-либо					
Да	32	15	30	17	34
Нет	68	35	70	33	66
7. Побуждение к курению, употреблению алкоголя, жестоким или опасным действиям					
Да	36	17	34	19	38
Нет	64	33	66	31	62
Всего:	100	50	100	50	100

8. Как Вы относитесь к «Интернет-пиратству»?	Всего абсолютные	Возраст 14-18 абсолют	Возраст 14-18 в %	Возраст 19-24 абсолют	Возраст 19-24 в %
1. Положительно, это позволяет получить бесплатный доступ к играм, кни	32	11	22	21	42
2. Скорее, положительно. Это вынужденное средство. Лицензионный дост	14	6	12	8	16
3. Скорее, отрицательно это нарушает права тех, кто владеет лицензией.	21	10	20	11	22
4. Отрицательно. Это нарушение закона.	33	23	46	10	20
Всего:	100	50	100	50	100

9. Какими средствами обеспечения информационной безопасности Вы пользуетесь?	Всего абсолютные	Возраст 14-18 абсолют	Возраст 14-18 в %	Возраст 36-56 абсолют	Возраст 19-24 в %
1. Антивирусные программы	58	28	33	30	35
2. Антиспамовые фильтры	36	16	19	20	24
3. Средства идентификации и электронные ключи	32	19	22	13	15
4. Межсетевые экраны	23	12	14	11	13
5. Средства авторизации	19	9	11	10	12
Другое	2	1	1	1	1
Всего:	100	50	100	50	100

10. Как Вы считаете, должны ли Вы заниматься обеспечением своей информационной безопасности?	Всего абсолютные	Возраст 14-18 абсолют	Возраст 14-18 в %	Возраст 19-24 абсолют	Возраст 19-24 в %
1. Да, каждый человек должен заботиться о своей информационной безопа	69	33	66	36	72
2. Нет, этим должны заниматься специальные государственные службы	16	9	18	7	14
3. Затрудняюсь ответить	15	8	16	7	14
Всего:	100	50	100	50	100

11. Какова, по Вашему мнению, эффективность следующих мер обеспечения информационной безопасности?	Всего абсолютные	Возраст 14-18 абсолют	Возраст 14-18 в %	Возраст 19-24 абсолют	Возраст 19-24 в %
1.Информирование молодёжи о правовых актах, обеспечивающих безопасность в информационной сфере					
0 баллов	7	3	6	4	8
1 балл	3	0	0	3	6
2 балла	2	1	2	1	2
3 балла	14	5	10	9	18
4 балла	18	11	22	7	14
5 балла	56	30	60	26	52
2.Работа государственных и правоохранительных органов по профилактике преступлений в информационной среде					
0 баллов	6	3	6	3	6
1 балл	3	0	0	3	6
2 балла	5	2	4	3	6
3 балла	15	8	16	7	14
4 балла	25	11	22	14	28
5 балла	46	26	52	20	40
3. Раскрытие преступлений, связанных с использованием информационных технологий					
0 баллов	6	3	6	3	6
1 балл	3	0	0	3	6
2 балла	7	3	6	4	8
3 балла	20	11	22	9	18
4 балла	23	10	20	13	26
5 балла	41	23	46	18	36
4. Ограничение доступа молодёжи к информационным ресурсам, представляющим опасность					
0 баллов	9	5	10	4	8
1 балл	5	0	0	5	10
2 балла	7	1	2	6	12
3 балла	16	12	24	4	8
4 балла	22	8	16	14	28
5 балла	41	24	48	17	34
5. Формирование информационной и коммуникативной компетентности молодёжи					
0 баллов	9	5	10	4	8
1 балл	1	0	0	1	2
2 балла	9	5	10	4	8
3 балла	20	7	14	13	26
4 балла	22	11	22	11	22
5 балла	39	22	44	17	34
Всего:	100	50	100	50	100

12. Насколько Вы информированы о средствах обеспечения государством информационной безопасности?	Всего абсолютные	Возраст 14-18 абсолют	Возраст 14-18 в %	Возраст 19-24 абсолют	Возраст 19-24 в %
1. Государственный контроль (контроль почтовых отправлений, телеграфных и иных сообщений, прослушивание телефонных переговоров при осуществлении оперативно-розыскных мероприятий)					
Информирован хорошо	63	33	66	30	60
Информирован не достаточно	30	13	26	17	34
Не информирован	7	4	8	3	6
2. Запрет на пропаганду террористической деятельности					
Информирован хорошо	52	23	46	29	58
Информирован не достаточно	37	21	42	16	32
Не информирован	10	6	12	4	8
3. Защита персональных данных					
Информирован хорошо	60	26	52	34	68
Информирован не достаточно	32	19	38	13	26
Не информирован	8	5	10	3	6
4. Защита права на собственное изображение					
Информирован хорошо	55	31	62	24	48
Информирован не достаточно	30	11	22	19	38
Не информирован	15	8	16	7	14
5. Разработка нормативно- правовых актов по обеспечению информационной безопасности					
Информирован хорошо	46	25	50	21	42
Информирован не достаточно	43	19	38	24	48
Не информирован	11	6	12	5	10
Всего:	100	50	100	50	100

13. Какие знания, по Вашему мнению, могут способствовать повышению информационной безопасности?	Всего абсолютные	Возраст 14-18 абсолют	Возраст 14-18 в %	Возраст 19-24 абсолют	Возраст 19-24 в %
1. О правах личности	59	27	18	32	22
2. О способах защиты прав личности	54	23	15	31	20
3. О наказаниях за преступления в информационной сфере	53	26	18	27	18
4. О факторах, угрожающих жизни, здоровью	60	37	25	23	15
5. О криминальной ситуации	36	18	12	18	12
6. О защите от информации, представляющей опасность для жизни, здоровья	38	19	12	19	13
7.Другое	0	0	0	0	0
Всего:	100	50	100	50	100

14. Как Вы оцениваете меры, предпринимаемые государством для обеспечения информационной безопасности?	Всего абсолютные	Возраст 14-18 абсолют	Возраст 14-18 в %	Возраст 19-24 абсолют	Возраст 19-24 в %
1. Эффективные	58	33	66	35	58
2. Недостаточно эффективные	22	10	20	12	20
3. Неэффективные	9	1	2	8	14
4. Затрудняюсь оценить	11	6	12	5	8
Всего:	100	50	100	50	100

15. Пожалуйста, укажите Ваш пол.	Всего абсолютные	Возраст 14-18 абсолют	Возраст 14-18 в %	Возраст 19-24 абсолют	Возраст 19-24 в %
1.Мужской	50	25	50	25	50
2.Женский	50	25	50	25	50
Всего:	100	50	100	50	100

16. Пожалуйста, укажите Ваш возраст	Всего абсолютные	Возраст 14-18 абсолют	Возраст 14-18 в %	Возраст 19-24 абсолют	Возраст 19-24 в %
1. 14-18 лет	50	25	50	25	50
2. 19-24 лет	50	25	50	25	50
Всего:	100	50	100	50	100

17. Оцените материальное положение Вашей семьи	Всего абсолютные	Возраст 14-18 абсолют	Возраст 14-18 в %	Возраст 19-24 абсолют	Возраст 19-24 в %
1. Выше среднего (чаще всего не имеем материальных затруднений)	39	19	38	20	40
2. Среднее (иногда испытываем материальные трудности)	50	23	46	27	54
3. Ниже среднего (приходится на многом экономить)	11	8	16	3	6
Всего:	100	50	100	50	100

Приложение 4

Вопросы интервью

1. Как Вы будете действовать, если обнаружите, что на Вашем компьютере появился вирус?
2. Пользуетесь ли Вы торрент- трекерами, если да, то для каких целей?
3. Как Вы относитесь к блокировке торрент- трекеров?
4. С какими угрозами информационной безопасности Вам приходилось сталкиваться в Интернете?
5. Какую информацию о себе Вы бы не стали распространять в Интернете?
6. Какие меры Вы предпринимаете для защиты своих данных в Интернете?
7. Как Вы относитесь к тому, что специальные службы могут собирать, хранить и просматривать Вашу переписку или любые другие личные данные, в качестве способа обеспечения общественной безопасности?
8. Как Вы считаете, какая персональная информация представляет для Интернет- мошенников наибольший интерес?
9. Насколько Вы доверяете информации, распространённой в Интернете?
10. Какие источники информации Вы считаете наиболее достоверными?
11. Как Вы действуете, когда видите рекламу в Интернете? Воспринимаете ли её всерьёз или не обращаете внимание?
12. На Ваш взгляд, распространение какого типа информации в Интернете может оказать негативное влияние на молодёжь?
13. Как Вы относитесь к использованию нелицензионного программного обеспечения?
14. Какое значение для Вас имеет сохранность Вашей личной информации?
15. Как Вы считаете, от кого в первую очередь зависит информационная безопасность человека?