ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»
(Н И У « Б е л Г У »)

ИНСТИТУТ УПРАВЛЕНИЯ
КАФЕДРА СОЦИОЛОГИИ И ОРГАНИЗАЦИИ РАБОТЫ С МОЛОДЕЖЬЮ

ПОВЫШЕНИЕ УРОВНЯ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МОЛОДЕЖИ

Выпускная квалификационная работа
обучающегося по направлению подготовки
39.03.03 Организация работы с молодежью
очной формы обучения, группы 05001411
Почапского Александра Михайловича

Научный руководитель
старший преподаватель
Говоруха Н.С.

БЕЛГОРОД 2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы выпускной квалификационной работы. Научно-техническая революция, начавшаяся в середине XX века, как результат превращения науки в ведущий фактор производства, послужила переходу от индустриального общества в постиндустриальное – в век информатизации общества. Последние десятилетия ознаменовались стремительностью и глобальностью развития информационных технологий. Компьютер, Интернет, электронная почта, социальные сети, цифровое телевидение и прочие мультимедийные устройства прочно заняли первое место среди интересов молодежи.

Молодежь – самая подверженная влиянию группа населения. Это обусловлено рядом факторов. Во-первых, молодые люди и девушки большую часть своего времени проводят среди различной информации: общаются в социальных сетях, смотрят фильмы, видеоролики, загружают программное обеспечение для своего ноутбука или планшета, играют в онлайн игры и многое другое.

Еще одним немаловажным фактором является юношеский максимализм. В 15-20 лет молодежь особенно трепетно относится к проблемам, воспринимает информацию больше эмоционально, нежели рационально. Поэтому чаще всего влиянию информационных угроз подвержена молодежь, желающая незамедлительных изменений.

В-третьих, все новое и неизведанное вызывает у молодых людей желание попробовать. Поэтому любое новое течение, навеянное модой, воспринимается положительно, так как это такая прекрасная возможность выразить свою точку зрения в информационном поле Интернета.

Он стал местом распространения различного вида угроз против охраняемых законом важнейших интересов социума. Актуальность информационных угроз и кибератак растет. Генеральная прокуратура РФ выявляет рост числа экстремизма в Интернете. По данным ФСБ, в Интернете представлены почти все международные террористические организации,

которые публикуют свои документы более чем на 40 языках[1]. Министр внутренних дел РФ В.Колокольцев отмечает, что «деструктивные силы, в том числе экстремистской направленности, все активнее используют ресурсы сети «Интернет» для организации и ведения информационно-психологической обработки граждан, пропаганды своих идей, привлечения новых членов, поисков источников финансирования»[2].

Все вышеперечисленное ставит перед обществом новую проблему – повышение культуры информационной безопасности молодежи в быстро меняющемся информационном обществе, в мире, где ускоряется процесс появления различных угроз, постоянно возникает потребность в обеспечении безопасности.

Степень научной разработанности темы исследования. Со второй половины XX-го столетия информационная безопасность является объектом научных исследований. Первые разработки в этой области связаны с исследованиями специалистов по вопросам компьютерной безопасности стран Запада в 1960-х годах. Из многочисленного ряда теоретических исследований проблем информационной безопасности выделим работы Г. Джоуэтта, Д. Робертсона, Ф. Уэбстера и др.[3], изучающих различные аспекты воздействия информации на процессы в международных отношениях.

Отечественная научная мысль обратила внимание на проблемы информационной безопасности в 90-е годы XX века в рамках обеспечения национальной безопасности государства, преодоления технологической и научно-технической зависимости Российской Федерации от внешних источников. Последние два десятилетия характеризуются интенсивным изучением данной области.

---

[1]ФСБ предсказывает террористические кибератаки. URL: http://www.securitylab.ru/news/377958.php (дата обращения: 20.09.2017).

[2]Там же.

[3]Джоуэтт Г.С. Пропаганда и внушение. М., 1988. С. 31-33; Робертсон Д. С. Информационная революция. М., 1992. С. 17-27; Уэбстер Ф. Теории информационного общества. М., 2004. С. 47-52.

Общая тематика исследований, рассматривающих проблемы применения информационных технологий, в научной литературе представлена технологическим и гуманитарным направлением решения задач информационной безопасности. В отличие от технологического подхода, разрабатывающего программно-техническую сторону процесса обеспечения информационной безопасности, гуманитарный рассматривает информационную безопасность в качестве междисциплинарной области научного знания, выделяя юридические, социологические и психологические аспекты указанного феномена.

Технологиям обеспечения информационной безопасности посвящены работы В.А. Васенина, Д.П. Зегжды, А.А. Малюка, А.В. Старовойтова, М.П. Сычева, Н.Г. Шурухнова, В.Н. Ясенева и др.[1] Авторы рассматривают технические приемы и методы обеспечения защиты компьютерной информации и информационных систем.

Междисциплинарная проблематика информационной безопасности является предметом исследований А.Н. Асаула, А.В. Возженникова, И.А. Лазарева, А.И. Позднякова и др.[2], синтезировать гуманитарную и техническую составляющие информационной безопасности пытаются Г.Г. Почепцов, С.П. Расторгуев и др.[3], социологические и политологические аспекты проблемы раскрываются в работах Г.Л. Смоляна, Д.С. Черешкина

---

[1]Васенин В.А. Информационная безопасность и компьютерный терроризм. М., 2004; Зегжда П.Д. Теория и практика обеспечения информационной безопасности. М., 1996; Малюк А.А. Введение в защиту информации в автоматизированных системах. М., 2001; Старовойтов А.В. Информационное обеспечение государственного управления. М., 2000; Сычев М.П. Киберпреступность и подготовка специалистов по борьбе с ней в России. М., 2005; Шурухнов Н. Г. Расследование неправомерного доступа к компьютерной информации. М., 1999; Ясенев В. Н. Информационная безопасность в экономических системах. Н. Новгород, 2006.

[2]Асаул А. Н. Организация предпринимательской деятельности. СПб., 2009; Возженников А. В. Основные концептуальные положения безопасности России в XXI веке. М., 2000; Лазарев И. А. Информационная безопасность. М., 1997; Поздняков А. И. Информационная безопасность личности, общества и государства. М., 1993.

[3]Почепцов Г.Г. Информационно-психологическая война. М., 2000; Расторгуев С. П. Информационная война. Проблемы и модели. Экзистенциальная математика. М., 2006.

и др.[1] Они обосновывают положение о том, что состояние информационной безопасности такой социальной системы, как общество, непосредственным образом зависит от обеспечения потребностей и интересов социальных групп и человека. Согласно их точке зрения, путь к безопасности находится только в единстве основных сфер жизни общества.

Различные аспекты защиты личности от негативного информационного воздействия раскрывают труды Ю.А. Ермакова, И.Н. Панарина, а также других авторов[2]. В этом ключе выделяется психологическое направление в исследованиях Г.В. Грачева, В.Н. Лопатина, И.К. Мельника, В.Д. Цыганкова[3], вопросам правовой защиты интересов личности, общества и государства посвящены работы А.А. Антопольского, И.Л. Бачило, В.Д. Попова, А.А. Фатьянова и т.д.[4] Исследования проблем информационной безопасности гуманитарного характера базируются на изучении общеметодологических основ процесса информационной безопасности, закономерностей развития информационной среды как системообразующего фактора жизни общества, путей и способов использования информационной сферы для реализации основных социально-политических задач России и т.д.

Кроме этого, необходимо отметить, что концептуальное понимание безопасности в социологии и философии исследуется в работах

---

[1]Смолян Г. Л. Сетевые информационные технологии и проблемы безопасности личности. М., 1999; Черешкин Д. С. Нелегкая судьба российской информатизации. М., 2008.

[2]Ермаков Ю. А. Манипуляция личностью: смысл, приёмы, последствия. Екатеринбург, 1999; Панарин А. С. Стратегическая нестабильность в XXI веке. М., 2003.

[3]Грачев Г. В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты. М., 1998; Лопатин В. Н. Безопасность – информационный выбор России в XXI в. М., 2003; Мельник И. К. Манипулирование личностью: организация, способы и технологии информационно-психологического воздействия. М., 2002; Цыганков В. Д. Психотроника и безопасность России. М., 2003.

[4]Антопольский А. А. Ответственность за правонарушения при работе с конфиденциальной информацией. М., 2001; Бачило И. Л. Информационное право: основы практической информатики. М., 2001; Попов В. Д. Парадигмы исследования информационных процессов. М., 2010; Фатьянов А. А. Информация как объект права. М., 2001.

Н.П. Ващекина, М.И. Дзлиева, А.Д. Урсула и др.[1] Существенный вклад в изучение проблем развития и применения информационных технологий в информационном обществе вносят труды Ю.Ф. Абрамова, С.Н. Гриняева, Г.В. Емельянова, К.К. Колина, А.Н. Кочергина, Н.Н. Моисеева, А.И. Ракитова, Г.Л. Смоляна и др.[2], а также Ж. Бодрийяра, М. Вебера, У. Дайзарда, П. Друкера и др., посвященные социально-философскому анализу информационных технологий как доминанте развития современного общества. Работы указанных авторов содержат анализ основных тенденций эволюции мирового социума. Авторы изучают описываемые проблемы с точки зрения перспектив развития человеческой цивилизации.

Определяющее значение для развития исследований философско-этической составляющей современного социума имеют работы Р.Г. Апресяна, В.И. Бакштановского, А.А. Гусейнова, В.Н. Назарова, Ю.В. Согомонова и других ученых[3], посвященные проблемам этики и морали российской действительности.

Проведенный анализ исследования в настоящее время требует своего решения. В настоящее время данная проблема не достаточно полно изучена, что повышает значимость исследования. Тема дипломного исследования носит проблемный характер.

Проблема исследования заключается в противоречии между наличием угроз в сети Интернет и способах повышения культуры информационной безопасности молодежи.

---

[1]Ващекин Н.П. Безопасность и устойчивое развитие России. М., 1998; Дзлиев М. И. Проблемы безопасности: теоретико-методологические аспекты. М., 2001; Урсул А. Д. Природа информации (Философский очерк). М., 1968.

[2]Абрамов Ю. Ф. Информационная цивилизация: природа и перспективы развития. Иркутск, 1998; Гриняев С. Н. Поле битвы – киберпространство: теория, приемы, средства, методы и системы ведения информационной войны. Минск, 2004; Емельянов Г. В. Проблемы обеспечения информационно-психологической безопасности России. М., 1999.

[3]Апресян Р.Г. Идея морали и базовые нормативно-этические программы. М., 1995; Бакштановский В.И. Честная игра: Нравственная философия и этика предпринимательства. Томск, 1992; Гусейнов А.А. Золотое правило нравственности. М., 1988; Назаретян А.П. Агрессия, мораль и кризисы в развитии мировой культуры. М., 1996; Назаров В.Н. Прикладная этика. М., 2005.

Объектом исследования выступает информационная безопасность молодежи.

Предметом исследования являются методы повышения культуры информационной безопасности молодежи.

Целью исследования является разработка проекта, направленного на повышение культуры информационной безопасности молодежи.

Задачи исследования:

1. Теоретическое обоснование проблемы информационной безопасности молодежи.

2. Анализ проблем информационной безопасности молодежи Белгородской области и разработка проекта по решению выявленных проблем.

3. Описание мероприятий проекта по формированию культуры информационной безопасности молодежи Белгородской области.

Теоретико-методологические основы исследования. Теоретическая основа исследования представлена теориями, посвященными решению актуальных вопросов процесса обеспечения информационной безопасности (А.В. Манойло, А.И. Поздняков, А.В. Тонконогов и др.)[1], изучению глобальных проблем современности, информационного противостояния (С.Н. Гриняев, С.П. Петров, С.П. Расторгуев и др.)[2], философии информационной цивилизации и теории информационного общества (А.И. Ракитов, М. Кастельс, А.Д. Урсул и др.)[3] .

---

[1]Манойло А.В. Государственная информационная политика в особых условиях. М., 2003; Поздняков А.И. Информационная безопасность страны и Вооруженных Сил // Национальная безопасность: актуальные проблемы. 1999. № 3; Тонконогов А.В. Информационно-психологическая безопасность в системе духовной безопасности современной России // Власть. 2012. № 6.

[2]Гриняев С.Н. Интеллектуальное противодействие информационному оружию. М., 1999; Петров В.П. Информационная безопасность человека и общества. М., 2007; Расторгуев С.П. Информационная война. Проблемы и модели. Экзистенциальная математика. М., 2006.

[3]Ракитов А.И. Информационная революция как фактор экономического и социального развития // Информационная революция: наука, экономика, технология. 1992.

Среди отечественных авторов, идеи которых способствовали конкретизации гуманитарных аспектов обеспечения информационной безопасности необходимо отметить А.Е. Войскунского, И.Л. Галинскую, А.А. Малюка и О.Ю. Полянскую и др.[1] Важнейшую теоретическую базу работы сформировали исследования, отражающие философские представления о процессе использования информационных технологий: теория информационной этики Н. Винера, учение о межкультурной информационной этике Р. Капурро, концепция моральной ответственности Г. Ленка и др.[2]

Методологической основой исследования является совокупность таких подходов, как системный, синергетический, исторический и т.д. Герменевтический подход открыл возможность расширить границы предметного поля информационной безопасности, синергетический метод позволил рассмотреть защиту безопасности как сложно функционирующее явление, диалектический метод раскрыл процесс обеспечения информационной безопасности в единстве с ценностным сознанием общества. В исследовании конкретного текстологического материала применены также общенаучные методы познания: анализ, синтез и др.

Эмпирическая база исследования:

1. Социологическое исследование «Безопасность персональных данных». Левада-Центр. Число участников опроса – 1600. Личное интервью с

№ 5; Кастельс М. Информационная эпоха: экономика, общество и культура. М., 2000; Урсул А.Д. Природа информации (Философский очерк). М., 1968.

[1]Войскунский А.Е. Информационная безопасность: психологические аспекты // Национальный психологический журнал. 2010. № 1(3); Галинская И.Л. Этико-правовое пространство информационно-компьютерных технологий // Новые инфокоммуникационные технологии в социально-гуманитарных науках и образовании: современное состояние, проблемы, перспективы развития. 2003. № 2; Малюк А.А. Гуманитарные аспекты информационной безопасности, образование, система подготовки специалистов в области информационной безопасности // Вестник РГНФ. 2011. № 4(65).

[2]Винер Н. Кибернетика, или управление и связь в животном и машине. М., 1958; Капурро Р. Информационная этика // Информационное общество. 2010. Вып. 5.

респондентами в возрасте 18 лет и старше в 137 населенных пунктах 48 регионов страны. 7-10 апреля 2017 г.[1]

2. Социологическое исследование «ВЦИОМ-Спутник». Число участников опроса – 2400. Телефонное интервью с респондентами в возрасте от 18 лет и старше на территории РФ. Декабрь 2017 г.[2]

3. Было проведено также авторское исследование «Определение уровня информационной безопасности молодежи». Выборка – серийная (гнездовая). Число участников опроса – 154 респондентов. Анкетный опрос молодежи Белгородской области, февраль-март 2018 г.

4. Использовались также данные Росстата об угрозах в сфере информационной безопасности[3].

Научно-практическая значимость исследования. Идеи и выводы, содержащиеся в работе, могут использоваться в дальнейших исследованиях по данной проблеме в философии науки и техники. Выводы исследования расширяют представления о содержании процессов обеспечения информационной безопасности, конкретизируют научные представления о ценностном потенциале формирующегося общества, способствуют более глубокому пониманию основ социокультурной трансформации и определению перспектив его развития. Материалы данного исследования могут быть использованы в образовательном процессе при подготовке учебных пособий, разработке курсов по социальной безопасности молодежи и ряда других дисциплин.

Апробация результатов исследования:

---

[1]Безопасность персональных данных. URL: https://www.levada.ru/2017/05/25/bezopasnost-personalnyh-dannyh/ (дата обращения: 23.09.2017).

[2]ВЦИОМ-Спутник. URL: https://wciom.ru/index.php?id=236&uid=116691 (дата обращения: 23.09.2017).

[3]Информационное общество в Российской Федерации. 2017: Стат. сб. / Росстат. М., 2017.

1. Статья: «Российский и зарубежный опыт формирования культуры информационной безопасности молодежи». Издательство «СибАК». Новосибирск, 2018 г.[1]

2. Статья: «Результаты социологического исследования «Определение уровня информационной безопасности молодежи». Издательство «СибАК». Новосибирск, 2018 г.[2]

Структура выпускной квалификационной работы. Данная работа состоит из введения, трех глав, заключения, списка источников и литературы, и приложений.

[1]Российский и зарубежный опыт формирования культуры информационной безопасности молодежи. URL: https://sibac.info/studconf/science/xxxix/98286 (дата обращения: 25.04.2018).

[2]См. Приложение 6.

ГЛАВА I. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ИССЛЕДОВАНИЯ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МОЛОДЕЖИ

1.1. Теоретическое обоснование проблемы информационной безопасности молодежи

Научно-техническая революция, начавшаяся в середине XX века, как результат превращения науки в ведущий фактор производства, послужила переходу от индустриального общества в постиндустриальное – в век информатизации общества. Последние десятилетия ознаменовались стремительностью и глобальностью развития информационных технологий. Компьютер, Интернет, электронная почта, социальные сети, цифровое телевидение и прочие мультимедийные устройства прочно заняли свое место среди интересов молодежи. Информационные технологии оказывают на молодое поколение неоднозначное воздействие. Процесс построения социальных взаимодействий в информационной среде, не основывающийся на культуре информационной безопасности, порождает отрицательное поведение у молодежи.

Выпускная квалификационная работа опирается на следующие понятия: культура, информационная безопасность, культура информационной безопасности, кибербезопасность, молодежь.

В информационном обществе основополагающим фактором развития является производство и использование человеком разнообразной информации. Следует отметить теорию постиндустриального общества. Основы данной теории заложил американский социолог Д. Белл[1], его идеи получили дальнейшее развитие в концепции «Трех волн» Э. Тоффлера[2].

Д. Белл заводит разговор о необходимости законодательного регулирования в области обеспечения свободного доступа к информации, устранение угрозы политического и административного контроля над

[1]Белл Д. Грядущее постиндустриальное общество. М., 1999. С. 18-22.
[2]Тоффлер Э. Третья волна. М., 1999. С. 36-38.

социальными субъектами через использование информационных технологий.

Продолжая развивать взгляды Д. Белла, Э. Тоффлер рассматривает эволюцию постиндустриального общества с точки зрения роста возможностей техники, а также ее влияния на движение социальных процессов в социуме[1]. Развитие технологий в человеческом обществе, по мнению Э. Тоффлера, имеет сходство с волнами, среди которых выделяются три основные. Технологические волны изменений затрагивают в первую очередь аграрную революцию, после – индустриальную и постиндустриальную революцию. Изучение нового общества во взаимодействии и целостности его сторон и т.д., внимательное отношение к нормативным ориентациям и ценностным критериям, относятся к основным достоинствам работы Э. Тоффлера. Он более выразительно описал, чем другие социальные философы, важную особенность грядущей социальной парадигмы. Это все нарастающее понимание, что человечество приблизилось к невиданным преобразованиям. Автор считает, что в скором будущем образование новых общественных отношений будет складываться на основе формирования объединений людей на определенных территориальных автономиях на основе различных интересов. Произойдет это благодаря новым технологиям, которые помогут в строительстве самостоятельного образа жизни. Потребность в неквалифицированном труде исчезнет, одновременно с тем возрастает потребность в специалистах, способных работать с техникой.

Особого внимания заслуживает также работа У. Дайзарда, описывающая сценарии перехода к информационному обществу и, сопровождающие данный процесс, возможные проблемы в сфере информационной безопасности[2]. Автор теории, изучая переход к информационному обществу, выделяет, что достигнутый уровень технологии

[1]Тоффлер Э. Третья волна. М., 1999. С. 38-42.

[2]Дайзард У. Наступление информационного века. Новая технократическая волна на Западе. М., 1986. С. 142-145.

в лице информационно-коммуникационных ресурсов предлагает ранее неизведанные возможности человечеству. По его мнению, отчетливо вырисовывается общая модель изменений, заключающая в себе три стадии:

- развитие экономических отраслей, связанных с производством и распределением информации,
- увеличение числа информационных услуг, ориентированных на обеспечение промышленности и правительства,
- формирование массовой информационной сети для широкого потребителя[1].

У. Дайзард начинает говорить о грядущих проблемах информационной безопасности: необъятные возможности новой технологии таят в себе не одну опасность, бороться с которыми человечеству придется каждый день.

Это может быть раздражающая путаница с кредитными картами, телефонные звонки и т.д. В результате чего может сложиться смутное беспокойство, от того, что техника переступила некоторую черту, за которой нет обратного пути. Данное беспокойство неумолимо нарастает от увеличения затрат энергетических ресурсов, защиты окружающей среды от загрязнения, в которых технологическая революция выступает скорее в роли причины их возникновения.

Таким образом, анализ формирования нового общества, осознание его в целостности, совместно с информационными технологиями, побуждает к поиску путей безопасного развития, преодолению негативных эффектов от применения информационных технологий, пересмотру ценностных ориентиров.

Культура – это исторически определённый уровень развития общества и человека. Термин «информационная культура» в отечественных публикациях впервые появился в 70-х годах XX века; инициаторами развития и популяризации соответствующей концепции стали работники

[1]Дайзард У. Наступление информационного века. Новая технократическая волна на Западе. М., 1986. С. 142-145.

библиотек. Одними из первых работ, в которых использовался этот термин, были статьи библиографов К.М. Войханской и Б.А. Смирновой «Библиотекари и читатели об информационной культуре» и Э.Л. Шапиро «О путях уменьшения неопределенности информационных запросов».

В настоящее время информационную культуру все чаще трактуют как особый феномен информационного общества. В зависимости от объекта рассмотрения стали выделять информационную культуру общества, информационную культуру отдельных категорий потребителей информации (например, детей или юристов) и информационную культуру личности.

Понятие «информационная культура» характеризует одну из граней культуры, связанную с информационным аспектом жизни людей. Роль этого аспекта в информационном обществе постоянно возрастает; и сегодня совокупность информационных потоков вокруг каждого человека столь велика, разнообразна и разветвлена, что требует от него знания законов информационной среды и умения ориентироваться в информационных потоках. В противном случае он не сможет адаптироваться к жизни в новых условиях, в частности, к изменению социальных структур, следствием которого будет значительное увеличение числа работающих в сфере информационной деятельности и услуг.

В настоящее время существует множество определений информационной культуры. В широком смысле под информационной культурой понимают совокупность принципов и реальных механизмов, обеспечивающих позитивное взаимодействие этнических и национальных культур, их соединение в общий опыт человечества.

В узком смысле – оптимальные способы обращения со знаками, данными, информацией и представление их заинтересованному потребителю для решения теоретических и практических задач; механизмы совершенствования технических сред производства, хранения и передачи информации; развитие системы обучения, подготовки человека к эффективному использованию информационных средств и информации.

Один из ведущих отечественных специалистов в области информатизации Э.П. Семенюк под информационной культурой понимает информационную компоненту человеческой культуры в целом, объективно характеризующую уровень всех осуществляемых в обществе информационных процессов и существующих информационных отношений.

Информационная культура личности – одна из составляющих общей культуры человека, совокупность информационного мировоззрения и системы знаний и умений, обеспечивающих целенаправленную самостоятельную деятельность по оптимальному удовлетворению индивидуальных информационных потребностей с использованием как традиционных, так и новых информационных технологий.

Специалисты выделяют следующие критерии информационной культуры человека:

- умение адекватно формулировать свою потребность в информации;
- эффективно осуществлять поиск нужной информации во всей совокупности информационных ресурсов;
- перерабатывать информацию и создавать качественно новую;
- вести индивидуальные информационно-поисковые системы;
- адекватно отбирать и оценивать информацию;
- способность к информационному общению и компьютерную грамотность.

Всё выше перечисленное должно базироваться на осознании роли информации в обществе, знании законов информационной среды и понимании своего места в ней, владении новыми информационными технологиями.

При этом информационная культура личности реализуется по уровням:

1. когнитивный уровень – знания и умения;
2. эмоционально-ценностный – установки, оценки, отношения;
3. поведенческий – реальное и потенциальное поведение.

Информационная культура организации рассматривается в рамках мировой информационной культуры, информационной культуры социальных институтов национальных государств и индивидов.

Информационную культуру изучают на следующих уровнях:

1. Микроуровень – информационная культура индивидов.

2. Мезоуровень – информационная культура организаций.

3. Макроуровень – информационная культура социальных институтов, регионов и государств.

4. Мегауровень – мировая (глобальная) информационная культура.

Информационная культура существует в неразрывном единстве, и феномены одного из уровней находят свое отражение на других уровнях. Носителями информационной культуры на различных уровнях являются Интернет-сообщество, население национальных государств, наемные работники, отдельные индивиды.

Оказывают влияние на информационную культуру следующие субъекты: транснациональные корпорации-производители ИТ, социальные институты, руководители организаций и индивиды. Информационная культура организации рассматривается на мезоуровне, но некоторые особенности информационной культуры персонала задаются на макроуровне (государственные и региональные образовательные программы, доступность ИТ для населения, уровень информатизации социальных институтов) и на мегауровне (новые возможности ИТ требуют новых навыков, соблюдения «правил игры» и другого отношения к ИТ). Однако в основе информационной культуры организации лежит индивидуальная информационная культура каждого работника.

В Доктрине информационной безопасности РФ под информационной безопасностью понимается состояние защищенности ее национальных

интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства[1].

Под культурой информационной безопасности понимается определенный уровень развития человека или общества, проявляемый в информационной сфере. Ю.В. Бородакий, А.Ю. Добродеев и И.В. Бутусов дали следующее понятие кибербезопасности: «кибербезопасность – это свойство или состояние системы сохранять надежность и функциональную устойчивость в условиях современного информационного противоборства» 2.

При определении понятия «культура информационной безопасности» мы отталкивались от исследований, проведенных А.А.Демидовым[3], А.А.Малюком[4], Л.В.Астаховой[5]. Под культурой информационной безопасности молодежи мы будем понимать процесс создания состояния защищенности молодежи, включающее в себя качественную информационную среду (защищенность от негативных информационных воздействий) и процесс создания защищенности их информации и обеспечивающее полное удовлетворение информационных потребностей молодежи.

При организации, проведении и проверке эффективности комплекса занятий по формированию культуры информационной безопасности молодежи можно использовать основные компоненты структуры культуры информационной безопасности школьников, а именно:

---

[1]Доктрина информационной безопасности РФ / Совет безопасности РФ. URL: http://www.scrf.gov.ru/documents/5.html (дата обращения: 29.10.2017).

[2]Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века // Вопросы кибербезопасности. 2013. № 1. С. 27-30.

3 Демидов А. А. Медиаобразование – комплексное решение проблем медиакомпетентности личности. Через медиаграмотность или через культуру информационной безопасности. URL: http:// www.pandia.ru/text/ 78/361/630.php (дата обращения: 21.09.2017).

4 Малюк А.А. Формирование культуры информационной безопасности общества // Педагогика. 2009. № 3. С. 33-39.

5 Астахова Л. В. Проблемы формирования культуры информационной безопасности в регионе // Социокультурные аспекты развития регионов: сб. науч. тр. / М-во образования и науки Челяб. обл.; Челяб. ин-т экономики и права им. М. В. Ладошина; [редкол.: С. Г. Зырянов и др.]. Челябинск, 2009. С. 206.

- когнитивный (знаниевый) компонент,
- компонент информационной культуры личности,
- коммуникативный компонент,
- компонент информационной защиты,
- компонент профилактики компьютерной и Интернет-зависимости,
- деятельностный компонент.

Когнитивный (знаниевый) компонент структуры культуры информационной безопасности рассматривается нами как наличие или отсутствие знания по культуре информационной безопасности.

Когнитивный опыт личности как компонент содержания общего образования и базовой культуры включает в себя систему знаний о природе, обществе, мышлении, технике, способах деятельности, и отражает процессы переработки информации: анализ поступающей информации, формализация, сравнение, обобщение, синтез с имеющимися знаниями, разработка вариантов использования информации и прогнозирование последствий реализации решения проблемной ситуации, генерирование и прогнозирование использования новой информации и взаимодействие ее с имеющимися знаниями.

Под компонентом информационной культуры личности мы понимали умение молодежи ориентироваться в потоках информации, оперативно оценить полезность информации и в дальнейшем целенаправленно и сознательно использовать ее при решении поставленных задач, для удовлетворения своей информационной потребности.

Коммуникативный компонент включает реальное и виртуальное общение молодежи, культуру общения и реализуется в общении и взаимодействии с другими людьми, в реальной жизни и/или в социальных сетях (Интернет) с применение языков и иных видов знаковых систем, технических средств коммуникаций в процессе передачи информации от одного человека к другому.

Компонент информационной защиты можно рассматривать с нескольких сторон:

1. Информационно-психологическая сторона: защита личности от информации, от негативного информационного воздействия; психологическая самозащита личности.

Основным законодательным документом, в котором прописана защита ребенка от информации, защита от негативного информационного воздействия, является Федеральный закон Российской Федерации от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

2. Техническая сторона: защита информации: использование технических средств для защиты информации.

Компонент профилактики компонент профилактики компьютерной и Интернет-зависимости.

Деятельностный компонент направлен на применение культуры информационной безопасности школьником в любом роде деятельности, будь то учебная, профессиональная или любая другая.

Опыт практической деятельности, анализ научной литературы показывает, что формирование культуры информационной безопасности молодежи должно иметь непрерывный характер, что обусловлено процессами глобальной информатизации, постоянным совершенствованием средств информационных и коммуникационных технологий, а также постоянно меняющимися условиями развития системы образования. Вместе с тем культура информационной безопасности может формироваться как на внеурочных мероприятиях, так и в процессе учебной деятельности, поэтому на этапе обучения необходимо предусмотреть последовательное решение конкретных задач по формированию культуры информационной безопасности молодежи.

Повышение культуры информационной безопасности молодежи – комплексное явление, включающее технические, этические и правовые

аспекты. В социуме информация распространяется быстро. Сама информация часто носит неоднозначный, недоброжелательный и негативный характер и влияет на социально-нравственные ориентиры общества. Разрушение духовной сферы общества в виде неправильных нравственных постулатов, ложных ориентаций и ценностей, оказывают влияние на состояние и всех сфер общественной жизни. В связи с этим, возникает проблема информационной безопасности, без решения которой не представляется возможным полноценное развитие не только личности, но и общества. Молодежь, включенная в процесс познания, оказывается беззащитной перед потоками информации[1]. В результате чего, возникает острая необходимость расширения образования молодежи, введения компонентов, связанных с обучением культуры информационной безопасности. Сегодня данная проблема становится все более актуальной.

Один из возможных путей разрешения проблемы информационной безопасности – обучение молодежи разумному восприятию и оценке информации, ее критическому обдумыванию на основе ценностей. И школьникам, и родителям необходимо знать о том, что в виртуальном мире существует целый свод правил[2], которыми нужно руководствоваться при работе и общении в сети. Тем не менее, информационная культура комплексна: она включает в себя различные элементы.

---

[1]Грачев Г.В. Информационно-психологическая безопасность личности: теория и технология психологической защиты: автореф. дис. ... д-ра психол. наук. М., 2000. С. 14-18.

[2]Плешаков В.А. Киберсоциализация человека: от Homo Sapiens’a до Homo Cyberus’a. М., 2011. С. 19-23.

1.2. Опыт формирования культуры информационной безопасности молодежи

Автором был проведен поиск и анализ статистического показателя, который бы позволил прямо или косвенно судить о проблеме развития информационных технологий и их негативным влиянием на молодежь[1]. Исследование, проведенное Левада-Центром, было посвящено безопасности персональных данных от 25.05.2017. Опрос проведен 7-10 апреля 2017 года по репрезентативной всероссийской выборке городского и сельского населения среди 1600 человек в возрасте 18 лет и старше в 137 населенных пунктах 48 регионов страны. Исследование проводилось на дому у респондента методом личного интервью. Распределение ответов приводится в процентах от общего числа опрошенных вместе с данными предыдущих опросов.

Рисунок 1. Вопрос «Информированы ли Вы о возможном получении личных данных пользователя хакерами при использовании мобильным телефоном и Интернетом?»

На вопрос об информированности населения о возможном получении личных данных пользователя хакерами при использовании мобильным

[1]Безопасность персональных данных. URL: https://www.levada.ru/2017/05/25/bezopasnost-personalnyh-dannyh/ (дата обращения: 23.09.2017).

телефоном и Интернетом в сравнении между январем 2012 года и апрелем 2017 года, число осведомленных выросло, количество не осведомленных снизилось. Общая же обеспокоенность касательно этого вопроса возросла (Рисунок 1). Количество пользователей, предпринимающих различные способы защиты личной информации выросло, а бездействующих снизилось.

На вопрос о причинах бездействия защиты персональной информации в динамике январь 2012 – апрель 2017, несколько выросло число респондентов, не видящих смысла в защите персональной информации. Количество воздержавшихся также несколько выросло (Рисунок 2).

Рисунок 2. Вопрос «Назовите причины бездействия защиты персональной информации»

На вопрос о необходимости деанонимизации в социальных сетях в динамике за январь 2012, март 2014 и апрель 2017 количество согласных увеличилось примерно вдвое, количество несогласных несколько снизилось. Число неопределившихся также снизилось (Рисунок 3).

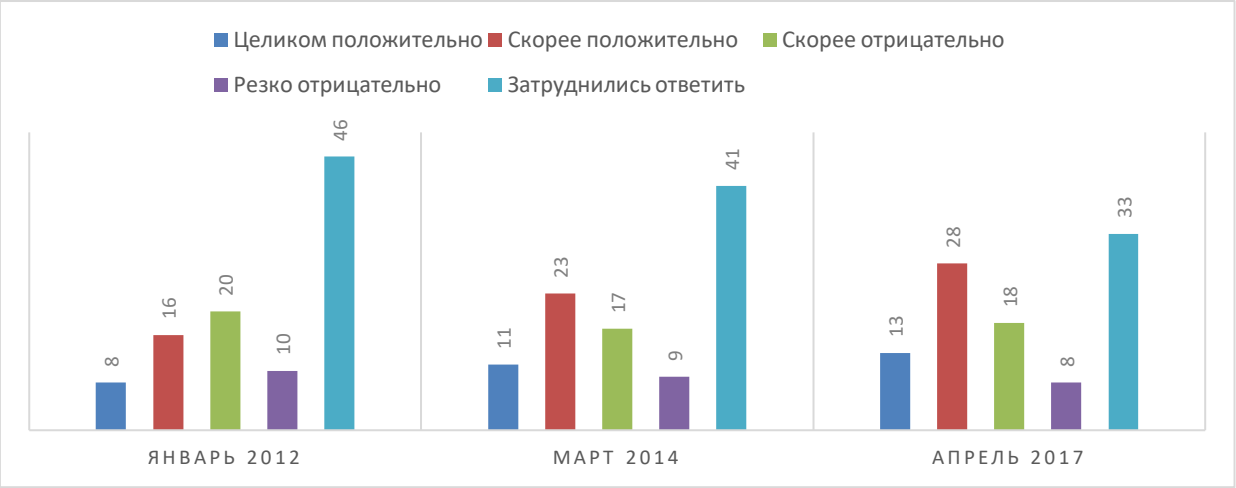

Рисунок 3. Вопрос «Необходима ли деанонимизация в социальных сетях?»

Таким образом, на основе данного исследования можно сделать вывод о том, что число заинтересованных респондентов в повышении информационной безопасности выросло, а количество безучастных граждан снизилось. Актуальность темы эмпирической базой исследования ВКР подтверждена.

Международный опыт решения проблемы информационной безопасности будет представлен системами Великобритании, ЕС и США. В Великобритании уделяется большое внимание культуре информационной безопасности как части медиакомпетентности граждан, целью которой является способность использовать медиа в личных целях и без посторонней помощи, понимать и критически оценивать различные аспекты медиа как таковые и содержание медиа, передавать (независимо от контекста), создавать и распространять медиатексты. Кроме того, в Великобритании существует целый ряд профессиональных организаций, в функции которых входит обеспечение информационной безопасности граждан: Управление по телекоммуникациям (OFCOM), Центр по борьбе с эксплуатацией и защите детей в Интернете (CEOP), Ассоциация медиаобразования Англии и Уэльса (MEA), Шотландская ассоциация медиаобразования (AMES) и другие. По данной проблематике реализуются различные проекты, например, межнациональный проект «Дети Европы Онлайн» (EU Kids Online),

исследующий опыт работы детей в Интернете, а также вопросы риска и интернет-безопасности.

Начиная со второй половины 90-х годов XX века в США серьезно задумались над повышением культуры информационной безопасности молодежи в сети Интернет. В октябре 1998 года бывший президент Бил Клинтон подписал закон «Акт о Защите Прав Детей в сети Интернет», который Конгресс ввел в исполнение в 2000 году. В США просвещение школьников основывается на встраиваемость информации, посвященной культуре информационной безопасности в школьную программу. Цель медиаобразования в США – научить школьников критически мыслить, находить различную информацию и использовать в своих целях. Так, на занятиях «Обществоведение» анализируются способы медийных манипуляций, применяемые политиками и террористами, освещение новостей различными СМИ, проблемы взаимодействия медиа и аудитории. Изучая предмет «Охрана здоровья» (Health), школьники рассматривают темы, связанные с рекламой продуктов питания, сигарет, алкоголя и лекарств и т.д.

В России также проводятся различные мероприятия в сфере информационной безопасности. Однако сейчас ясно выделились два решения в данной сфере.

Первое решение представляет собой поиск нежелательной информации в Интернете добровольцами и обращение в Роскомнадзор с целью ее блокирования. В этом случае молодежь выступает как активный инструмент воздействия – субъект. На сегодняшний момент времени данное решение оформилось в кибердружины. Данная структура была создана Лигой безопасного Интернета в 2011 году. Лига – это крупнейшая в России организация, созданная для противодействия распространению опасного контента во всемирной сети. Лига безопасного интернета была учреждена в 2011 году при поддержке Минкомсвязи РФ, МВД РФ, Комитета Госдумы РФ по вопросам семьи, женщин и детей. Попечительский совет Лиги возглавляет

помощник Президента Российской Федерации Игорь Щеголев. Целью лиги является искоренение опасного контента путем самоорганизации профессионального сообщества, участников интернет-рынка и рядовых пользователей. «Кибердружина» – межрегиональное молодежное общественное движение, которое объединяет более 20 тысяч добровольцев со всей России и стран СНГ, борющихся с преступлениями в виртуальной среде. «Кибердружина» имеет представительства в 36 регионах России. Площадкой для «живого» общения кибердружинников служит ежегодный Всероссийский слет активистов движения «Кибердружина». Традиционно он проходит в Москве и собирает сотни кибердружинников[1]. В Белгородской области деятельность кибердружин регламентирует Постановление правительства Белгородской области от 22. 05. 2017 года № 181-пп «Об организации деятельности кибердружин Белгородской области». Существует группа социальной сети ВКонтакте от г. Старый Оскол[2].

Второе решение представляет собой просвещение молодежи в сфере информационных технологий, заключающееся в объяснении ей способов защиты от вредной информации. В этом случае молодежь выступает в качестве объекта воздействия, поглощая предоставляемую учителями, организаторами работы с молодежью информацию. Данное направление развития характеризуется своей «молодостью» и инновационностью. Первым, кто задумался об Интернет-безопасности, стал Региональный общественный центр интернет-технологий. Свою деятельность он ведет с 2007 года. Начало берется с Урвана Парфентьева и Марка Твердынина, которые посещали международные конференции, и подняли проблему Интернет-безопасности в России.

[1]Кибердружина. URL: http://www.ligainternet.ru/liga/activity-cyber.php (дата обращения: 23.09.2017).

[2]Кибердружина. Старый Оскол. URL: https://vk.com/kiberdruzhin.oskol (дата обращения: 23.09.2017).

Во-первых, это предоставление покрытия Интернета в регионах. Реализуется это благодаря Ростелекому. Осуществляется это для различных целей, одной из которых является поиск пропавших без вести.

Во-вторых, это образовательная деятельность в рамках учреждений. Например, «Единый урок информационной безопасности в сети Интернет». В данном комплексе мероприятий участвуют 36286 школ и более 12 миллионов учащихся. Инициатива была выдвинута В.И. Матвиенко, спикером Совета Федерации, в рамках парламентских слушаний на тему «Актуальные вопросы обеспечения информационной безопасности детей при использовании ресурсов сети Интернет» 14 марта 2014 года. Проект представляет собой образовательную деятельность со школьниками, студентами ВУЗов и СПО, а также с родителями. Также Фонд Развития Интернет с МТС создал «Урок полезного и безопасного Интернета». Количество участников более 320 000 из 30 регионов России.

В-третьих, образовательная деятельность в сети Интернет. Ведет активную деятельность и Координационный центр доменов RU/.РФ. Проекты для детей и школьников «Изучи Интернет – управляй им!», всероссийский онлайн-чемпионат для школьников (15 тысяч участников). «Позитивный контент» – конкурс сайтов для детей. Также Яндекс реализует онлайн-проект «Сетевичок». Создана Интернет-среда, содержащая в себе информацию для детей с доменом .ДЕТИ. ДЕТИ является социально направленным проектом. Миссия домена .ДЕТИ заключается в повышении цифровой грамотности детей и подростков, объединении качественного интернет-контента. Другая важная задача – сделать пребывание детей в интернете комфортным и безопасным. В домене .ДЕТИ уже работают сайты детских садов, школ, учреждений дополнительного образования и досуга.

В-четвертых, используется технология телефонного и онлайн-консультирования. Фондом Развития Интернет совместно с компаниями МГТС и МТС была запущена линия помощи (8-800-25-000-15 и helpline@detionline.com с 9:00 до 18:00 по московскому времени) в 2009 году.

Целевой аудиторией являются дети, подростки и работник образовательных и воспитательных учреждений. На Линии помощи «Дети Онлайн» работают профессиональные эксперты-психологи Фонда Развития Интернет и выпускники факультета психологии МГУ имени М.В. Ломоносова.

В-пятых, ведется разработка учебно-методической литературы, посвященной безопасности в сети Интернет. Так, Фонд Развития Интернет с МТС В 2013 году разработали методическое пособие «Интернет: возможности, компетенции, безопасность» для работников системы общего образования. Целевой аудиторией пособия являются ученики средней школы. В 2016 году совместно с Роскомнадзором было подготовлено пособие «Практическая психология безопасности: управление персональными данными в Интернете» для работников системы общего образования. Пособие включает в себя практические занятия для 6-10 классов общеобразовательных школ и посвящено повышению цифровой компетентности школьников и учителей в сфере управления персональными данными в Интернете[1].

Ведется работа и на региональном уровне. Наиболее активным представителем является Республика Татарстан. Так, Правительство Татарстана утвердило план мероприятий по обеспечению информационной безопасности детей в медиапространстве на 2017-2019 годы. Своей целью Правительство Татарстана видит «повышение духовно-нравственной культуры» молодых людей (до 23 лет), формирование у них «позитивной картины и адекватных базисных представлений об окружающем мире и человеке», навыков «самостоятельного и ответственного потребления информационной продукции»[2]. В Белгородской области также активно развивается направление информационной безопасности молодежи. Так, на сайте Департамента образования Белгородской области активно реализуется

---

[1]Единый урок безопасности // Фонд Развития Интернет. 2017. № 26. С. 10-14.

[2]Татарстанскую молодёжь защитят от интернета. URL:https://www.idelreal.org/a/28664674.html (дата обращения: 23.09.2017).

проект «Безопасное детство»[1]. Целью данного проекта является повышение компетенций «Безопасное детство» учащихся, родителей и педагогов в не менее чем 400-х общеобразовательных учреждениях к декабрю 2018 года на территории Белгородской области. Также, на сайте МБОУ «Хотмыжской СОШ» подробно расписан план реализации проекта[2] в разделе «Информационная безопасность».

Согласно проекту Концепции стратегии кибербезопасности РФ[3] данная проектная идея имеет отношение к направлению № 7: Формирование и развитие культуры безопасного поведения в киберпространстве и безопасного использования его сервисами, а именно: организация комплексной информационной кампании в целях повышения уровня информированности граждан, организаций и государственных органов об актуальных киберугрозах, уязвимостях защищаемых ресурсов в киберпространстве и способах их компенсации, популяризация доступных технологий, мер и средств обеспечения кибербезопасности. Данная проектная идея, в отличии от идеи проекта «Безопасное детство», ограничена возрастными рамками молодежи в пределах 14–20 лет. Это связано с тем, что исследовательская служба GfK констатировала, что в России, начале 2015 года, 89% подростков пользуется Интернетом в возрасте 12-17 лет[4]. Суть проблемы заключается в том, что современная молодежь недостаточно хорошо осведомлена в знании и поведении в рамках информационного общества. На основе статистических данных, представленных в эмпирической базе исследования ВКР, можно сделать вывод о том, что необходимость в повышении культуры информационной безопасности молодежи высока.

---

[1]Безопасное детство. URL: https://образование31.рф/our-projects/information-security-of-children-and-adolescents/ (дата обращения: 23.09.2017).

[2]Информационная безопасность. URL: http://hotmijskou.net/elektron_servise/Telefoni.htm (дата обращения: 23.09.2017).

[3]Проект Концепции стратегии кибербезопасности РФ. URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 23.09.2017).

[4]Бочаров М.П., Чумиков А.Н,. Самойленко С.А. Реклама и связи с общественностью: профессиональные компетенции. М., 2016. С. 48-52.

Проектная идея автора выпускной квалификационной работы представляет собой проведение цикла мероприятий, направленных на повышение уровня культуры информационной безопасности. Данный цикл представляет собой комплекс занятий, включающий в себя лекции с интерактивными элементами, проведение уроков, оценка уровня информационной безопасности молодежи.

В течение цикла мероприятий будут применяться механизмы учета статистических данных для определения достижения участниками цели проекта. Цель, результат и остальная информация будет указана в плане и паспорте проекта. Особенность данного цикла мероприятий обуславливается тем, что весь цикл прекрасно будет применяться в различных образовательно-досуговых центрах: школах, ВУЗах, центрах молодежных инициатив и т.д.

Новизна проекта имеет 5 уровень: использование опыта районов и повторение проекта на разных территориях одного региона. Таким образом, изучив опыт решения проблемы, можно сделать вывод о том, что проект целесообразен.

1.3. Анализ законодательства в области формирования культуры информационной безопасности молодежи

Анализ законодательства в сфере построения информационного общества и информационной безопасности без рассмотрения международного аспекта международной нормативно-правовой законодательной базы был бы невозможен. Рассмотрим основные из них.

Основополагающим документом является Окинавская хартия глобального информационного общества (Окинава, 22 июля 2000 г.)[1]. На создание данного документа повлияла теория Е. Масуды – японского ученого в сфере информационных технологий. Подписали данный документ страны, входившие на тот момент времени в G8. «Восьмерка» провозгласила основные положения, согласно которым информационные технологии (ИТ) считаются одним из важнейших факторов развития современного общества. Таким образом, Окинавская хартия являет собой важнейший документ, призванный организовать и активизировать деятельность стран и правительств на пути активного формирования глобального информационного общества планеты.

Также следует отметить Конференции по информационной безопасности, прошедшие под эгидой ООН и соответствующие документы: Декларация принципов и План действий. Всемирный саммит по информационному обществу (Женева, 12 декабря 2003 г.)[2] и Тунисская программа для информационного общества (Тунис, 18 ноября 2005 г.)[3]. Документы, принятые в Женеве, закладывают фундамент жизни в информационном обществе, установлены ограниченные временными

[1]Окинавская Хартия глобального информационного общества. URL: http://www.kremlin.ru/supplement/3170 (дата обращения: 03.10.2017).

[2]Декларация принципов и План действий. URL: http://library.zntu.edu.ua/zakon/03declar.html (дата обращения: 03.10.2017).

[3]Тунисская программа для информационного общества. URL: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/bc 05d17935b393aac32575a8004cd760 (дата обращения: 03.10.2017).

рамками цели, достижение которых будет способствовать претворению в реальность концепции открытого для всех и справедливого информационного общества. Тунисская программа стала катализатором программ, принятых в Женеве, а также существенно их дополнив в области распространения информации в мире и защите пользователей от недобросовестной информации.

Немаловажно следует отметить документы, регулирующие законодательство по вопросам сохранения информации и доступа к ней. Хартия о сохранении цифрового наследия (принята на 32-й Генеральной конференции ЮНЕСКО. Париж, октябрь 2003)[1]. Международная конвенция об охране нематериального культурного наследия (Париж, 17 октября 2003 г.)[2]. Стратегический план программы ЮНЕСКО «Информация для всех» на 2008-2013 гг. (принят Исполнительным советом ЮНЕСКО на 180-й сессии 30 сентября – 17 октября 2008 г.)[3].

В начале 2000-х годов Пражская декларация «К информационно грамотному обществу» (2003) и Александрийская декларация об информационной грамотности и образовании на протяжении всей жизни (2005) подчеркнули значение информационной грамотности для устойчивого развития человечества и построения партисипативных и инклюзивных обществ в XXI веке и в дальнейший период. Информационная грамотность, рассматриваемая как неотъемлемая часть одного из основных прав человека: на образование на протяжении всей жизни, имеет решающее значение для

[1]Хартия о сохранении цифрового наследия. URL: http://www.ifap.ru/ofdocs/unesco/digit.htm (дата обращения: 03.10.2017).

[2]Конвенция об охране нематериального культурного наследия. URL: http://www.un.org/ru/documents/decl_conv/conventions/cultural_heritage_conv (дата обращения: 03.10.2017).

[3]Стратегический план программы ЮНЕСКО «Информация для всех» на 2008-2013 гг. URL: http://www.ifap.ru/ofdocs/unesco/sp813.pdf (дата обращения: 03.10.2017).

достижения целей развития тысячелетия ООН и соблюдения принципов Всеобщей декларации прав человека[1].

Согласно Александрийской декларации об информационной грамотности и образовании на протяжении всей жизни (2005) информационная грамотность – это способность человека выражать свои информационные потребности; находить и оценивать качество информации; хранить и извлекать информацию; осуществлять эффективное этическое использование информации; применять информацию для создания и обмена знаниями.

В 2011 году была принята Фесская декларация о медиа- и информационной грамотности, которая обратила внимание на необходимость объединение этих двух понятий.

Так, информационная грамотность включает следующие навыки:

1) выявление/осознание информационных потребностей;
2) выявление источников информации;
3) определение местоположения или поиск информации;
4) анализ и оценка качества информации;
5) организация, хранение или архивирование информации;
6) использование информации в соответствии с этическими нормами, эффективное и результативное;
7) создание и обмен новыми знаниями[2].

Следует также отметить основополагающие международные документы, касающиеся этических, правовых и социальных последствий использования информационных и телекоммуникационных сетей. Всеобщая декларация прав человека (Париж, 10 декабря 1948 г.)[3]. Всемирная

[1]Медиа- и информационная грамотность в обществе: материалы междун. конф. М., 2013. С. 33-35.

[2]Туоминен С., Котилайнен С. Педагогические аспекты формирования медийной и информационной грамотности. М., 2012. С. 42-48.

[3]Всеобщая декларация прав человека. URL: http://www.consultant.ru/document/cons_doc_LAW_120805/ (дата обращения: 03.10.2017).

конвенция об авторском праве (Женева, 6 сентября 1952 г.)[1]. Всеобщая декларация ЮНЕСКО о культурном разнообразии (резолюция принята по докладу Комиссии IV на 20-м пленарном заседании 2 ноября 2001 г.)[2]. Обобщающий документ Форума по вопросам управления Интернетом (Хайдерабад, 3-6 декабря 2008 г.)[3].

Теперь перейдем к рассмотрению российского законодательства в сфере информационных технологий и информационной безопасности. Основополагающим документом в сфере информационных технологий является Доктрина информационной безопасности РФ[4]. Она представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации. Доктрина понимает под информационной безопасностью Российской Федерации состояние защищенности национальных интересов России в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. Она закрепляет обязательное соблюдение конституционных прав и свобод человека в области получения информации и пользования ею. Также информационного обеспечения государственной политики России с доступом граждан к открытым государственным ресурсам. Немаловажными элементами развития информационных технологий в России являются развитие современных информационных технологий отечественной индустрии, обеспечение информационных технологий внутреннего рынка России и выход на мировые рынки. Уделяется внимание защите

[1]Всемирная конвенция об авторском праве. URL: http://docs.cntd.ru/document/1900510 (дата обращения: 06.10.2017).

[2]Всеобщая декларация ЮНЕСКО о культурном разнообразии. URL: http://www.un.org/ru/documents/decl_conv/declarations/cultural_diversity.shtml (дата обращения: 06.10.2017).

[3]Форум по вопросам управления Интернетом (ФУИ). Третье совещание. Обобщающий документ. URL:http://www.ifap.ru/pr/2008/n081201a.pdf (дата обращения: 06.10.2017).

[4]Доктрина информационной безопасности Российской Федерации. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 06.10.2017).

информационных ресурсов от несанкционированного доступа, обеспечению безопасности информационных и телекоммуникационных систем.

Законодательство России в сфере информационной безопасности развивается по следующим направлениям:

1. закрепление общих положений о доступе к информации, о конфиденциальности и защите информации. Базовым актом здесь является Федеральный закон «Об информации, информационных технологиях и защите информации»;

2. определение правового режима отдельных видов информации:

- персональных данных – Федеральный закон «О персональных данных»
- семейной тайны и тайны личной жизни – Гражданский и Семейный кодексы
- государственной тайны – Закон РФ «О государственной тайне»
- коммерческой тайны – Гражданский кодекс РФ и Федеральный закон «О коммерческой тайне»
- профессиональных, процессуальных тайн – процессуальными кодексами и законами о соответствующих видах деятельности (об адвокатуре, нотариате, охране здоровья граждан и т.п.);

3. административное регулирование деятельности по защите информации, в том числе связанной с оборотом криптографических средств;

4. определение порядка осуществления оперативно-розыскных мероприятий в информационной сфере;

5. борьба с преступлениями в сфере информационной безопасности путем закрепления соответствующих составов преступлений в Уголовном кодексе РФ.

Следует выделить следующие законодательные акты РФ:

1. Указ президента РФ «О Совете при Президенте РФ по развитию информационного общества в РФ» (№ 1576 от 1 ноября 2008 г.) и методические материалы, издаваемые Советом[1].

2. ФЗ «Закон о средствах массовой информации» от 27 декабря 1991 года № 2124-1[2].

3. ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» от 9 февраля 2009 г. № 8-ФЗ[3].

4. ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ[4].

5. Концепция правовой информатизации России (в редакции указов Президента РФ от 19.11.2003 г. № 1365: от 22.03.2005 г. № 329)[5].

6. ФЗ «О персональных данных» от 27 июля 2006 г. № 152-ФЗ[6].

Автор выпускной квалификационной работы, проанализировав перечень нормативной документации правового характера, необходимой для реализации проекта составил список юридических документов, необходимых для реализации определенного проекта:

1. Федеральный закон «Об образовании в РФ» № 273-ФЗ от 29 декабря 2012 года – используется в сфере общей нормативной документации,

---

[1]О Совете при Президенте РФ по развитию информационного общества в РФ: Указ Президента РФ № 1576 от 01.11.2008 г. // Российская газета. 2008. 14 ноября. С. 18-19.

[2]О средствах массовой информации: Федеральный Закон от 27 декабря 1991 года № 2124-1 // Российская газета. 2007. 28 ноября. С. 10-19.

[3]Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления (с изменениями и дополнениями): Федеральный Закон от 9 февраля 2009 г. № 8-ФЗ // Российская газета. 2009. 13 февраля. С. 10-19.

[4]Об информации, информационных технологиях и о защите информации (с изменениями и дополнениями): Федеральный Закон от 27 июля 2006 г. № 149-ФЗ // Российская газета. 2006. 29 июля. С. 6-16.

[5]О Концепции правовой информатизации России (с изменениями и дополнениями): Указ Президента РФ от 28.06.1993 г. № 966 // Российская газета. 1993. 03 июля. С. 12-18.

[6]О персональных данных: Федеральный Закон от 29 июля 2006 г. № 152-ФЗ. // Российская газета. 2006. 29 июля. С. 12-18.

необходимой для применения цикла мероприятий в учреждениях системы образования РФ.

2. Распоряжение Правительства Российской Федерации от 29 ноября 2014 г. № 2403-р «Об утверждении основ государственной молодежной политики Российской Федерации на период до 2025 года» – используется в сфере общей нормативной документации для применения цикла мероприятий в работе с молодежью.

3. Закон Белгородской области от 3 октября 2013 г. № 223 «О поддержке молодежи в Белгородской области» – используется в сфере общей нормативной документации для применения цикла мероприятий в работе с молодежью с учетом особенностей Белгородской области.

Специфические законодательные акты, регулирующие деятельность в сфере проектной документации:

4. ISO 21500 – 2014 «Руководство по проектному менеджменту» – международный стандарт в сфере проектного управления.

5. ГОСТ Р 54869 – 2011 «Требования к управлению проектом» – национальный стандарт в сфере проектного управления.

6. ГОСТ Р 54870 – 2011 «Требования к управлению портфелем проекта» – национальный стандарт в сфере проектного управления, регламентирующий документальное оформление проекта.

7. ГОСТ Р 54871 – 2011 «Требования к управлению программой проекта» – национальный стандарт в сфере проектного управления, регламентирующий документальное оформление проекта.

8. Постановление Правительства Белгородской области № 202-пп от 31 мая 2010 года «Об утверждении положения об управлении проектами в органах исполнительной власти и государственных органах Белгородской области» – стандарт Белгородской области в сфере проектного управления, учитывающий 4 предыдущих документа.

На основе изученного автором теоретического материала, необходимого для написания выпускной квалификационной работы, можно сделать следующие выводы:

1. Согласно, теориям развития информационного общества и информационной безопасности, можно заключить, что непрерывное развитие информационных технологии привело к вовлечению молодежи в информационную сферу, приобретению участникам данной сферы различных проблем: «поедание» времени, хакинг, мошенничество, развитие инфантилизма и т.д.

2. Общество, осознав силу влияния информационных технологий, пошло по просветительскому направлению: введение медиаобразования в школьную программу на Западе, организации уроков в России, направленных на повышение информационной грамотности учащихся. Также активно развивается и охранительное направление: создание «Кибердружин».

3. Законодательство в сфере информационных технологий начало свое развитие с 2000-х годов. Это обусловлено массовым распространением сети Интернет. Международные законодательные акты установили всеобщность информации, медиаграмотность и разграничение информации в Сети. Российское законодательство также не отстает в данном направлении. В последнее время в России активно развивается направление в сфере формирования информационной культуры и грамотности среди школьников.

ГЛАВА II. АНАЛИЗ ПРОБЛЕМЫ ПОВЫШЕНИЯ УРОВНЯ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МОЛОДЕЖИ И ЕЕ ПРОЕКТНОЕ РЕШЕНИЕ

2.1. Проблемное исследование целевых групп

Основываясь на анализе нормативной документации и эмпирической базе исследования нами предложены 6 критериев, уровни и показатели сформированности культуры информационной безопасности молодежи.

Таблица 1

Перечень критериев, уровней и показателей сформированности культуры информационной безопасности молодежи

Когнитивный критерий	
Низкий	Проявляет интерес к теме, но не видит личной заинтересованности; понимает термин и значение понятия «культура информационной безопасности»
Средний	Стремится к диалогическим взаимоотношениям с миром, знает нравственные законы, нормы, правила поведения; стремится к развитию, достижению хороших результатов, к творческой деятельности; осознает важность преимущественно личной информационной безопасности, в том числе и в сети Интернет; владеет разносторонними знаниями культуры информационной безопасности
Высокий	Имеет собственный практический опыт жизни, деятельности и общения; активно взаимодействует с миром; имеет результаты деятельности в виде творческих проектов и индивидуальных достижений; умеет выявлять опасности; в ситуации моделирования самостоятельной познавательной деятельности опасности локализуются, предотвращаются с использованием оптимального набора способов и средств обеспечения информационной безопасности
Критерий информационной культуры личности	
Низкий	Владеет навыками работы с каталогами и картотеками, книгами, периодическими изданиями; умеет упорядочивать, систематизировать, структурировать информацию; владеет навыками работы с текстом (культура чтения); знает способы представления информации в переработанном виде (реферат, аннотация, дайджест, конспект и т. д.)
Средний	Умеет анализировать, синтезировать и оценивать информацию (критическое мышление); владеет навыками работы в современных поисковых системах; владеет умениями и навыками конструктивного преобразования информации; владеет навыками использования инструментов информационно-поисковой деятельности
Высокий	Способен четко осознавать информационные потребности; умеет выявлять и оценивать источники информации; способен оценить эффективность процесса удовлетворения информационных

	потребностей; умеет представлять любую информацию в переработанном виде; умеет построить информационную модель поискового запроса и умеет анализировать эту модель с помощью автоматизированных информационных систем
Коммуникативный критерий	
Низкий	Умеет обмениваться сообщениями с людьми и в социальных сетях; умеет находить информацию по заданным критериям; умеет представить информацию в виде, понятном другим участникам
Средний	Знает виды каналов передачи информации в Сети и умеет ими пользоваться; умеет работать в информационной среде; знает нормы культуры общения; знает этику речевого и сетевого общения; умеет излагать, обсуждать и отстаивать свое мнение в формальной и неформальной обстановке, в письменной и устной форме
Высокий	Знает особенности информационных потоков по своей учебной деятельности; умеет пользоваться автоматизированными информационными системами сбора, хранения, переработки, передачи и представления информации, базирующимися на электронной технике и системах телекоммуникации; способен самостоятельно осуществлять поисковую и исследовательскую деятельность по учебе с использованием справочно-информационных сред и компьютерных справочников; - поведение отвечает нравственным нормам, что проявляется в интересе к знанию, познанию, в свободной коммуникации, бесконфликтному общению; умеет аналитически воспринимать письменную и устную информацию, включая адекватное восприятие культурных и языковых различий
Критерий информационной защиты	
Низкий	Знания о негативных информационных воздействиях носят бессистемный, отрывочный характер, знания по обеспечению информационной безопасности личности отсутствуют; - причины возникновения ситуаций негативного воздействия связывают только с плохой организацией информационной инфраструктуры, что мешает осознанию школьником своей активной роли в создании информационного пространства, принятию ответственности; умеет работать с антивирусными программами
Средний	Умеет анализировать и оценивать информацию (критическое мышление); умеет выявлять и нейтрализовать информационную угрозу, информационную опасность; знает и осознает личную ответственность за распространяемую информацию в социальных сетях; знает основные закономерности поведения человека в информационном обществе
Высокий	Знает основные законодательные и нормативные документы в области информационной безопасности личности; имеет внутренние принципы и убеждения, препятствующие распространению социально-деструктивной информации и дезинформации, манипулированию сознанием людей
Критерий зависимого поведения	
Низкий	Подвержен большому влиянию компьютера, Интернета. не представляет себе жизни без них; вытесняется реальный мир, меняется самосознание и самооценка под воздействием

	компьютера и Интернета
Средний	Способен контролировать себя и свои запросы, но уже есть зависимость; проводит много времени за компьютером и в Интернете, нахождение за компьютером принимает систематический характер
Высокий	Не подвержен серьезному влиянию Интернета и компьютера; отсутствует устойчивая потребность в компьютере и в выходе в Интернет
Деятельностный критерий	
Низкий	Информационная и компьютерная грамотность; умеет ориентироваться в информационных потоках; владеет методикой работы с традиционными и нетрадиционными источниками; вся работа по созданию проектов осуществляется только под руководством
Средний	Умеет использовать новые информационные технологии; умеет решать стандартные учебные задачи с помощью информационных технологий; вся работа по созданию проектов осуществляется под руководством
Высокий	Владеет приемами действий культуры информационной безопасности в нестандартных ситуациях для решения проблем; вся работа по созданию проектов осуществляется самостоятельно

Для выявления уровня информационной безопасности молодежи Белгородской области в феврале – марте 2018 года в рамках выпускной квалификационной работы нами было проведено социологическое исследование. В нем приняли участие 154 человека в возрасте от 18 до 30 лет, проживающих в Белгороде и 19 районах Белгородской области. 46,8% опрошенных – молодые люди и 53,2% – девушки. 59,7% респондентов обучаются в учебных заведениях СПО, 22,1% – в ВУЗах и 18,2% – работают.

В ходе исследования было выявлено следующее.

Под информационной безопасностью большинство опрошенных понимают обеспечение конфиденциальности информации (75,3%), по 11,7% набрали ответы: организация доступности информации для авторизованных пользователей и знания и умения, обеспечивающие регулирование информации (Приложение 3, Диаграмма 1). Как нам кажется, это обусловлено большим вниманием опрошенных к личным файлам, опасением компрометирования.

На необходимость правового регулирования в сфере информационной безопасности указало 88,3% участников опроса. Лишь 2,6 % респондентов

считают, что нет необходимости в правовом регулировании, затрудняются ответить 9,1% (Приложение 3, Диаграмма 2). Данные результаты свидетельствуют о том, что большинство молодых людей заинтересованы в защите персональной информации.

Для организации информационной безопасности 97,4% респондентов используют антивирусные средства (Приложение 3, Диаграмма 3), 42,9% – резервное копирование, 10,4% – системы бесперебойного питания. Как нам кажется, это обусловлено большой частотой использования сети Интернет и активным обменом различной информацией.

У большинства опрошенных программное обеспечение обновляется автоматически с получением уведомления (59,7%) и без получения уведомления (7,8%). 28,6% молодых людей обновляют программное обеспечение вручную. И только 3,9% респондентов не обновляют программное обеспечение (Приложение 3, Диаграмма 4). По нашему мнению, это обусловлено доверием автоматизации и нежеланием разбираться в обновлении самостоятельно, а также развитостью и популярностью систем автообновления программного обеспечения.

Процедуру аутентификации при использовании собственных устройств используют 81,8% респондентов. Не используют 10,4% молодых людей и 7,8% затруднились ответить (Приложение 3, Диаграмма 5). Как нам кажется, это обусловлено: а) желанием жить не публично, б) боязнью компрометирования, шантажа.

Самым распространенным способом аутентификации является код-пароль. Его используют 74,3% опрошенных, на втором и третьем месте отпечаток пальца (37,1%) и код-графический ключ (35,7%). Меньше всего используется дополнительный код (8,6%) (Приложение 3, Диаграмма 6). По нашему мнению, это обусловлено: а) защитой своего устройство максимально просто и надежно, б) техническим оснащением устройства, в частности, датчиками отпечатка пальца; в) привычкой использования того или иного способа.

Все опрошенные имеют аккаунт в социальных сетях (100%), причём 80,5% имеют несколько аккаунтов (Приложение 3, Диаграмма 7). Таким образом, по нашему мнению, это обусловлено: а) желанию обмена информацией, б) наличием свободного времени, в) стремлением «быть как все».

93,5% респондентов пользуются социальными системами несколько раз в день. Остальные опрошенные (6,5%) один раз в день (Приложение 3, Диаграмма 8). Таким образом, по нашему мнению, это обусловлено: а) желанию обмена информацией, б) наличием свободного времени, в) стремлением «быть как все».

Наиболее распространенной социальной сетью среди опрошенных является ВКонтакте. 100% молодых людей имеют в ней аккаунты. На втором месте Одноклассники (53,2%), на третьем месте – Telegram (40,3%) (Приложение 3, Диаграмма 9). Таким образом, по нашему мнению, это обусловлено: а) возможностью пользоваться библиотекой файлов ВКонтакте, б) возрастом опрашиваемой аудитории, в) популярностью Telegram, связанная с именем основателя ВКонтакте – Павлом Дуровым.

Среди социальных сетей чаще всего респонденты используют ВКонтакте (96,1%). 10,4% молодых людей используют Telegram, Instagram 9,1% (Приложение 3, Диаграмма 10). Как нам кажется, это обусловлено возрастом опрашиваемой аудитории и желанием обмена информацией.

Большинство опрошенных используют социальную сеть для общения по работе (учебе) – 76,6% и общения с досуговыми целями – 64,9%. Потребление контента в досуговых целях указали 35% респондентов (Приложение 3, Диаграмма 11). Как нам кажется, это обусловлено: а) наличием свободного времени, б) инфантилизмом, в) желанием пользоваться Интернетом.

63,6% респондентов проводят в Интернете более трех часов в день. До трех часов в день проводят в Интернете 18,2% опрошенных, до двух часов в день – 16,9% молодых людей (Приложение 3, Диаграмма 12). Как нам

кажется, это обусловлено: а) наличием свободного времени, б) инфантилизмом, в) желанием пользоваться Интернетом.

Большинство опрошенных используют Интернет для работы (учебы) – 85,7%, в досуговых целях – 64,9%. Социальные сети (мессенджеры) используют в Интернете 63,6% респондентов, электронной почтой пользуются 61% молодых людей (Приложение 3, Диаграмма 13). По нашему мнению, это обусловлено: а) необходимостью использовать Интернет в образовательных и рабочих целях, б) молодежь видит проведение своего досуга через использование сети Интернет.

При этом Интернет не является помехой при выполнении других задач, не связанных с Интернетом, для 42,8% опрошенных. Скорее не является помехой для 39% молодых людей. Частично является помехой для 10,4% респондентов (Приложение 3, Диаграмма 14). Как нам кажется, данный результат связан с интеграцией сети Интернет в процесс выполнения различных операций.

Большинство респондентов используют для выхода в Интернет смартфон – 89,6% и компьютер (ноутбук) – 72,7%. Планшет используют 15,6% респондентов (Приложение 3, Диаграмма 15). Как нам кажется, это обусловлено: а) мобильностью использования сети Интернет вне дома/учебы/работы, б) использованием компьютера (ноутбука) дома/на учебе/работе, в) громоздкостью использования планшета вне дома/учебы/работы.

Достоверность информации не проверяют 9,1% опрошенных. 75,3% пользуются проверенными источниками. Остальные ответы распределились следующим образом (Приложение 3, Диаграмма 16). По нашему мнению, это обусловлено доверием к определенным источникам и поиском различной информации.

Не пользуются образовательными интернет-порталами 35,1% опрошенных. Наиболее распространены следующие образовательные порталы: Edu.ru, GoogleScholar, eLibrary (по 27,3%) (Приложение 3,

Диаграмма 17). Как нам кажется, это обусловлено: а) незнанием об образовательных источниках, б) удовлетворенностью текущими знаниями, в) использованием только конкретных образовательных интернет-порталов.

Наиболее популярным интернет-порталом среди опрошенных является Российский Союз Молодёжи (46,8%). 40,3% респондентов не пользуются молодежными информационными интернет-порталами (Приложение 3, Диаграмма 18). По нашему мнению, это обусловлено: а) использованием только портала Российского Союза Молодежи, б) незнанием о существовании каких-либо еще молодежных интернет-порталов, в) незаинтересованностью в деятельности молодежных информационных порталов.

Уровень информационной безопасности большинство респондентов оценили хорошо (41,6%), удовлетворительно (38,9%) и отлично (10,4%). 9,1% опрошенных указали на неудовлетворительный уровень информационной безопасности (Приложение 3, Диаграмма 19). Как нам кажется, это связано с: а) личным опытом использования сети Интернет, б) информацией из различных СМИ.

Актуальность угроз в сфере информационной безопасности респонденты распределили следующим образом: мошенники, хакеры (58,4%), нежелательное содержание (50,6%), вредоносные и нежелательные программы (50,6%) (Приложение 3, Диаграмма 20). По нашему мнению, это обусловлено актуальностью встреч респондентов с данными угрозами в сети Интернет.

По мнению респондентов, молодежь подвержена угрозам в сфере информационной безопасности из-за отсутствия навыков противостояния мошенникам, хакерам (48,1%), также отсутствуют навыки самоконтроля и навыки планирования времени (46,8%), нет контроля со стороны родителей (45,5%) (Приложение 3, Диаграмма 21). Как нам кажется, это обусловлено: а) выборочной совокупностью респондентов (студенты ВУЗа и СПО), б) личному опыту и в) информацией из СМИ.

Повышать культуру информационной безопасности, по мнению респондентов, необходимо защитой персональных данных (61%), разработкой нормативно-правового законодательства в сети Интернет (44,2%), проведением различных курсов по информационной безопасности (41,6%) (Приложение 3, Диаграмма 22). По нашему мнению, это обусловлено: а) опасением компрометирования, б) опасением получения психологического и физического насилия, в) желанием противостоять различного рода воздействиям.

Таким образом, на основе проведенного социологического исследования можно сделать вывод о том, что большинство респондентов пользуются антивирусной защитой, используют аутентификацию в виде код-пароля, имеют несколько аккаунтов в социальных сетях/мессенджерах, среди которых ВКонтакте, Одноклассники и Telegram. Однако приоритетной социальной сетью является ВКонтакте. Социальные сети молодежь использует, в основном, для общения. Интернету большинство уделяет более 3 часов в день, потребляя контент для работы/учебы. При этом, для большинства респондентов, использование сети Интернет не оказывает влияния на другие дела. Большинство опрошенных пользуются проверенными источниками. Мнение молодежи разделилось насчет оценки уровня информационной безопасности между «хорошо» и «удовлетворительно». Повышение уровня культуры информационной безопасности большинство молодых людей видит в защите персональных данных.

2.2. Паспорт проекта «Организация комплекса мероприятий по повышению уровня культуры информационной безопасности»

УТВЕЖДАЮ:

Заместитель начальника департамента внутренней и кадровой политики области – начальник управления молодежной политики Белгородской области

/ Чесноков А.В./

М.П.

« » 2018 г.

УТВЕЖДАЮ:

Начальник отдела ОГБУ «ЦМИ»

/ Максимов П.В./

М.П.

« » 2018 г.

Паспорт проекта

Организация комплекса мероприятий по повышению уровня культуры информационной безопасности

Идентификационный номер_____

ПОДГОТОВИЛ

Студент группы 05001411
Институт управления НИУ «БелГУ»

/Почапский А.М. /

«___» _____ 2018 г.

Общие сведения о документе

Основание для составления документа:	постановление Правительства Белгородской области от 31 мая 2010 года №202-пп «Об утверждении Положения об управлении проектами в органах исполнительной власти и государственных органах Белгородской области»
Назначение документа:	регламентация взаимодействия между основными участниками проекта, закрепление полномочий и ответственности каждой из сторон реализации проекта
Количество экземпляров и место хранения:	выпускается в 3-х экземплярах, которые хранятся у руководителя проекта, куратора проекта и председателя экспертной комиссии по рассмотрению проектов
Содержание:	1. Группа управлением проектом 2. Основание для открытия проекта 3. Цель и результат проекта 4. Ограничения проекта 5. Критерии оценки и характеристика проекта
Изменения:	изменения в паспорт проекта вносятся путем оформления ведомости изменений

1. Группа управления проектом

Название и реквизиты организации	**ФИО, должность, контактные данные представителя**	**Наименование и реквизиты документа, подтверждающего участие представителя в проекте**
Координирующий орган: Управление молодежной политики по Белгородской области Телефон: (4722) 58-99-04 Адрес: Россия, 308023, Белгородская область, г. Белгород, ул. Студенческая, 17а	**Куратор проекта: Чесноков Андрей Валерьевич, заместитель начальника департамента внутренней и кадровой политики области – начальник управления молодежной политики Белгородской области** Телефон: (4722) 58-99-25 E-mail: depvkp@belregion.ru	**_____** **_____** **от «__» _____20___г. №_____**
Отдел информационно-аналитической работы управления молодежной политики по Белгородской области Телефон: (4722) 58-99-07 Адрес: Россия, 308023, Белгородская область, г. Белгород, ул. Студенческая, 17а E-mail: udmpr2009@yandex.ru	**Руководитель проекта: Почапский Александр Михайлович, студент 4-го курса ОРМ** Телефон: 8 920 558 99 23 E-mail: aleksandrpochapskiyy@rambler.ru	**от «__» _____20___г. №_____**

2. Основание для открытия проекта

2.1. Направление Стратегии социально-экономического развития Белгородской области:	Становление благоприятной социальной среды и создание условий для эффективной реализации человеческого потенциала и обеспечения качества жизни населения на основе динамичного развития экономики региона
2.2. Индикатор (показатель) реализации Стратегии социально-экономического развития Белгородской области:	• воссоздание окружающей среды, благоприятной для жизнедеятельности человека, повышение уровня безопасности населения области. • развитие духовного потенциала, улучшение качества человеческих отношений путем формирования регионального солидарного общества; • развитие институтов гражданского общества, повышение уровня самоорганизации общества, гражданской активности населения.
2.3. Наименование государственной программы Белгородской области **2.4. Наименование подпрограммы государственной программы Белгородской области**	Развитие образования Белгородской области на 2014-2020 годы Развитие дополнительного образования детей
2.5. Сведения об инициации проекта	Инициатор (ФИО, должность и контактные данные): студент Почапский Александр Михайлович Телефон: 89205589923 E-mail: aleksandrpochapskiyy@rambler.ru Дата регистрации: Формальное основание для открытия проекта: 14 февраля – День работника ЭВМ

3. Цель и результат проекта

<table>
<tr><td>3.1. Измеримая цель проекта:</td><td colspan="2">Организовать комплекс мероприятий на базе ЦМИ г. Белгород по повышению уровня культуры информационной безопасности для молодежи 14-20 лет до 28.04.18.</td></tr>
<tr><td>3.2. Способ достижения цели:</td><td colspan="2">Серия мероприятий:
1. Рассылка памятки, посвященной информационной безопасности.
2. Мониторинг социальной сети ВКонтакте на предмет противоправного контента («Кибердружина»).
3. Встреча, посвященная авторскому праву в сети Интернет.
4. Семинар, посвященный созданию контента в соответствии с авторским правом.
5. Встреча, посвященная опасностям сети Интернет.
6. Встреча, посвященная психологическим воздействиям в сети Интернет.
7. Цикл мероприятий в рамках учебно-методического пособия «Практическая психология безопасности: управление персональными данными в Интернете»[1].</td></tr>
<tr><td rowspan="4">3.3. Результат проекта:

3.4. Требования к результату проекта:
передача знаний, направленных на повышение культуры информационной безопасности не менее 30 учащимся.</td><td>Результат:
1. Привлечение в проект 50 участников.</td><td>Вид подтверждения:
1. Отчет о проделанной работе.</td></tr>
<tr><td>Требование:</td><td>Вид подтверждения:</td></tr>
<tr><td>Утверждена команда проекта</td><td>Копия утвержденного списка команды проекта</td></tr>
<tr><td>Утвержден список участников проекта</td><td>Копия утвержденного списка участников проекта</td></tr>
<tr><td></td><td>Реализован проект</td><td>Организована работа команды проекта. Проект начал свою реализацию.</td></tr>
<tr><td>3.5. Пользователи результатом проекта:</td><td colspan="2">Обучающиеся, студенты</td></tr>
</table>

1. обязательные требования к результату для экономических проектов

[1]Солдатова Г.У., Приезжева А.А., Олькина О.И., Шляпников В.Н. Практическая психология безопасности. Управление персональными данными в интернете: учеб.-метод. пособие для работников системы общего образования. М., 2017. С. 98-104.

4. Ограничения проекта

БЮДЖЕТ ПРОЕКТА (руб.):	
Целевое бюджетное финансирование:	
- федеральный бюджет:	• 0 руб.
- областной бюджет:	• 0 руб.
- местный бюджет:	• 0 руб.
Внебюджетные источники финансирования:	
- средства хозяйствующего субъекта:	• 16800 руб.
- заемные средства:	•
- прочие (указать): **Общий бюджет проекта:**	• Спонсорская помощь – 700 руб. • 17 500 руб.
СРОКИ РЕАЛИЗАЦИИ ПРОЕКТА (чч.мм.гг.)	
Дата начала проекта (план):	19.03.18
Дата завершения проекта (план):	28.04.18

5. Критерии оценки и характеристика проекта

КРИТЕРИИ УСПЕШНОСТИ ПРОЕКТА	
Наименование критерия	**Показатель**
Отклонение по бюджету (п.4)	Превышение на не более 875 руб. (5 %) относительно базового бюджета проекта соответствует 3-5% успешности проекта
Отклонение по срокам (п 4.); Достижение результата проекта (п. 3.3.);	Превышение на не более 2 дней относительно установленного срока окончания проекта соответствует 3-5% успешности проекта Наличие результата проекта соответствует 55% успешности проекта
Соблюдение требований к результату проекта (п. 3.4.);	Выполнение всех требований к результату проекта соответствует 3-5% успешности проекта

ХАРАКТЕРИСТИКА ПРОЕКТА	
Территория реализации проекта	ЦМИ , г. Белгород, ул. Студенческая, 17а
Уровень сложности проекта	Начальный
Тип проекта	Социальный

2.3. План проекта «Организация комплекса мероприятий по повышению уровня культуры информационной безопасности»

УТВЕЖДАЮ:

Заместитель начальника департамента внутренней и кадровой политики области – начальник управления молодежной политики Белгородской области

/ Чесноков А.В./

М.П.

« » 2018 г.

УТВЕЖДАЮ:

Начальник отдела ОГБУ «ЦМИ»

/ Максимов П.В./

М.П.

« » 2018 г.

План управления проектом

Организация комплекса мероприятий по повышению уровня культуры информационной безопасности

(полное наименование проекта)

Идентификационный номер_____

ПОДГОТОВИЛ

Студент группы 05001411
Институт управления НИУ «БелГУ»

/Почапский А.М. /

«___» _____ 2018 г.

Общие сведения о документе:

Основание для составления проекта:	Постановление Правительства Белгородской области от 31 мая 2010 года №202-пп «Об утверждения Положения об управлении проектами в органах исполнительной власти и государственных органах Белгородской области»
Назначение документа:	Детализация паспорта проекта и инициатива блока работ по планированию проекта, с точки зрения человеческих, финансовых и временных ресурсов
Количество экземпляров и место хранения:	Выпускается в 3-х экземплярах, которые хранятся у руководителя проекта, куратора проекта и председателя экспертной комиссии по рассмотрению проектов
Содержание:	1. Календарный план-график работ по проекту 2. Бюджет проекта 3. Участие области в реализации проекта 4. Риски проекта 5. Команда проекта 6. Планирование коммуникаций 7. Заинтересованные лица, инвесторы
Изменения:	Изменения в плане управления проекта выполняются путем оформления ведомости изменений

1. Календарный план-график работ по проекту

Код задачи	Название задачи	Длительность, дни	Дата начала работ	Дата окончания работ (контрольная точка)	Документ, подтверждающий выполнение работы	ФИО ответственного исполнителя
1.	Обсуждение идеи реализации проекта с руководителем практики от организации Максимовым П.В.	1	23.03.18	23.03.18	-	Почапский А.М.
2.	Разработка проектной документации и ее утверждение	9	22.03.18	31.03.18	Паспорт и план проекта. Экспертиза проекта	Почапский А.М.
3.	Мониторинг ВКонтакте на предмет противоправного контента в рамках прохождения производственной преддипломной практики от Кибердружины.	41	19.03.18	28.04.18	Характеристика от руководителя практикой	Почапский А.М.
4.	Рассылка памятки по информационной безопасности в рамках прохождения производственной преддипломной практики от Кибердружины.	1	02.04.18	02.04.18	Отчет	Почапский А.М.
5.	Встреча «Авторское право в сети Интернет» в рамках прохождения производственной преддипломной практики.	1	02.04.18	02.04.18	Отчет	Лектор
6.	Семинар «Создание контента, соответствующий Авторскому праву» в рамках прохождения производственной преддипломной практики.	1	04.04.18	04.04.18	Отчет	Тренер-фасилитатор
7.	Встреча «Опасности сети Интернет» в рамках прохождения производственной преддипломной практики.	1	06.04.18	06.04.18	Отчет	Лектор
8.	Встреча «Психологическое воздействие	1	09.04.18	09.04.18	Отчет	Лектор

	в социальных сетях» в рамках прохождения производственной преддипломной практики.					
9.	Мероприятие № 1. Что такое персональные данные? в рамках прохождения производственной преддипломной практики.	1	11.04.18	11.04.18	Отчет	Тренер-фасилитатор
10.	Мероприятие № 2. Какими бывают персональные данные? в рамках прохождения производственной преддипломной практики.	1	12.04.18	12.04.18	Отчет	Тренер-фасилитатор
11.	Мероприятие № 3. Как персональные данные попадают в сеть? в рамках прохождения производственной преддипломной практики.	1	13.04.18	13.04.18	Отчет	Тренер-фасилитатор
12.	Мероприятие № 4. Почему нужно управлять персональными данными? в рамках прохождения производственной преддипломной практики.	1	16.04.18	16.04.18	Отчет	Тренер-фасилитатор
13.	Мероприятие № 5. Как защитить персональные данные? в рамках прохождения производственной преддипломной практики.	1	17.04.18	17.04.18	Отчет	Тренер-фасилитатор
14.	Мероприятие № 6. Что такое приватность и личные границы? в рамках прохождения производственной преддипломной практики.	1	18.04.18	18.04.18	Отчет	Тренер-фасилитатор
15.	Мероприятие № 7. Как настраивать приватность в сети? в рамках прохождения производственной преддипломной практики.	1	20.04.18	20.04.18	Отчет	Тренер-фасилитатор
16.	Мероприятие № 8. Как управлять репутацией в сети? в рамках	1	23.04.18	23.04.18	Отчет	Тренер-фасилитатор

	прохождения производственной преддипломной практики.					
17.	Мероприятие № 9. Что мой смартфон знает обо мне? в рамках прохождения производственной преддипломной практики.	1	24.04.18	24.04.18	Отчет	Тренер-фасилитатор
18.	Мероприятие № 10. Как удалить персональные данные из интернета? в рамках прохождения производственной преддипломной практики.	1	25.04.18	25.04.18	Отчет	Тренер-фасилитатор
19.	Формирование плана мероприятий	3	28.03.18	31.03.18	Программа мероприятий	Почапский А.М.
20.	Проведение цикла мероприятий в рамках прохождения производственной преддипломной практики.	41	19.03.18	28.04.18	Письменный отчет	Почапский А.М.
21.	Оценка результатов проекта	1	28.04.18	28.04.18	Отчет о проделанной работе	Почапский А.М.
	Итого:	41				

2. Бюджет проекта

Код задачи	Название задачи	Сумма, руб.	Внебюджетные источники финансирования		
			средства хозяйствующего субъекта	заемные средства[1]	прочие[2]
1.	Мониторинг ВКонтакте	700	0	0	700
2.	Встреча «Авторское право в сети Интернет»	1200	1200	0	0
3.	Семинар «Создание контента, соответствующий Авторскому праву»	1200	1200	0	0
4.	Встреча «Опасности сети Интернет»	1200	1200	0	0
5.	Встреча «Психологическое воздействие в социальных сетях»	1200	1200	0	0
6.	Мероприятие № 1. Что такое персональные данные?	1200	1200	0	0
7.	Мероприятие № 2. Какими бывают персональные данные?	1200	1200	0	0
8.	Мероприятие № 3. Как персональные данные попадают в сеть?	1200	1200	0	0
9.	Мероприятие № 4. Почему нужно управлять персональными данными?	1200	1200	0	0
10.	Мероприятие № 5. Как защитить персональные данные?	1200	1200	0	0
11.	Мероприятие № 6. Что такое приватность и личные границы?	1200	1200	0	0
12.	Мероприятие № 7. Как настраивать приватность в сети?	1200	1200	0	0
13.	Мероприятие № 8. Как управлять репутацией в сети?	1200	1200	0	0
14.	Мероприятие № 9. Что мой смартфон знает обо мне?	1200	1200	0	0
15.	Мероприятие № 10. Как удалить персональные данные из интернета?	1200	1200	0	0
	Итого:	17500	**16800**	**0**	**700**

[1]следует указать источники заемных средств
[2]спонсорская помощь:

3. Риски проекта

№ п/п	Наименование риска проекта	Ожидаемые последствия наступления риска	Предупреждение наступления риска		Действия в случае наступления риска
			Мероприятия по предупреждению	ФИО ответственного исполнителя	
1.	Отсутствие людей на мероприятиях	Срыв сроков реализации проекта	Своевременное оповещение людей об анонсах мероприятий, уточнение их условий	Почапский А.М.	Приглашение обучающихся городских образовательных учреждений
2.	Некачественное содержание мероприятия	Снижения доверия к мероприятиям проекта	Тщательный отбор и проверка содержания материалов мероприятия	Почапский А.М.	Замена ведущего, замена контента
3.	Отказ в предоставлении помещения для проведения мероприятия	Закрытие проекта	Поиск альтернативных мест проведения мероприятия	Почапский А.М.	Проведение мероприятия в другом месте
4.	Отсутствие денег	Закрытие проекта	Поиск нескольких источников финансирования проекта	Почапский А.М.	Поиск спонсоров
5.	Сбой в работе техники на мероприятии	Снижения доверия к мероприятиям проекта	Подготовка дополнительного комплекта техники,	Почапский А.М.	Замена

5. Команда проекта

п/п	ФИО, должность и основное место работы	Ранг в области проектного управления	Роль в проекте/выполняемые в проекте работы	Трудо-затраты, дней	Основание участия в проекте
1.	Чесноков А.В.	Куратор	Координирует работу группы, помогают руководителю проекта решать возникающие вопросы с заинтересованными сторона	41	
2.	Максимов П.В.	Администратор	Ведет документацию по проекту, контролирует выполнение плана-графика проекта	41	
3.	Почапский А.М.	Руководитель	Руководит проектом, организует работу группы, отвечает за результат проекта	41	
4.	Говоруха Н.С.	Эксперт	Консультирует руководителя проекта по содержанию мероприятий проекта	41	
5.	Лектор	Исполнитель	Ведет лекции в рамках проекта	3	
6.	Тренер-фасилитатор	Исполнитель	Ведет тренинги в рамах проекта	12	
			ИТОГО:	220	

На основе изученного автором проектно-аналитического материала, необходимого для написания выпускной квалификационной работы, можно сделать следующие выводы:

1. В результате проведенного социологического исследования, результаты которого указаны в параграфе 2.1, говорят о востребованности проектной идеи. Экспертный опрос и экспертиза проектной идеи, указанные там же, подтверждают это. Благодаря им были внесены необходимые изменения.

2. Проектная идея имеет начальный уровень сложности, социальную направленность. Рассчитана на обучающихся старших классов, а также студентов.

3. Проектная идея включает в себя комплекс мероприятий, в том числе встречи, семинары. Подробнее будет изложено в параграфе 3.2. «Описание мероприятий проектной идеи». Данная система позволяет обеспечить максимально простую и ясную систему оценки уровня информационной безопасности молодежи.

Таким образом, можно подвести итоги проектно-аналитической части ВКР и перейти к 3 Главе.

ГЛАВА III. ОПИСАНИЕ МЕРОПРИЯТИЙ ПРОЕКТА «ОРГАНИЗАЦИЯ КОМПЛЕКСА МЕРОПРИЯТИЙ ПО ПОВЫШЕНИЮ УРОВНЯ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» И ОБОСНОВАНИЕ ЕГО ЭФФЕКТИВНОСТИ

3.1. Показатели реализации проекта «Организация комплекса мероприятий по повышению уровня культуры информационной безопасности» и его социально-экономической эффективности

Следует выделить качественные и количественные показатели реализации проекта «Организация комплекса мероприятий по повышению уровня культуры информационной безопасности» социально-экономической эффективности от внедрения проектного предложения.

Показатели:

1. Оценка текущего уровня информационной безопасности молодежи.

1) Разработка и проведение социсследования, определяющий уровень информационной безопасности у молодежи. Количественные: 154 респондента. Качественные: результаты уровня информационной безопасности молодежи. 2) Разработка и проведение экспертного опроса, определяющий уровень информационной безопасности у молодежи. Количественные: 10 экспертов. Качественные: оценка уровня информационной безопасности молодежи. Данные результаты можно использовать для планирования комплекса мероприятий, в том числе мониторинговых и образовательно-досуговых.

2. Поиск противоправного контента в сети Интернет.

1) Мониторинг ВКонтакте. Количественные: регистрация в месяц 100 случаев противоправного контента. Качественные: повышение сознательности пользователей социальной сети ВКонтакте, передача информации о противоправных действиях компетентным органам.

3. Организация досуговой деятельности по повышению уровня культуры информационной безопасности молодежи.

1) Комплекс мероприятий по информационной безопасности. Включает в себя:

1. Раздача памятки по информационной безопасности. Количественные: 50 листовок. Качественные: передача информации об угрозах в сфере информационной безопасности.

2. Встреча «Авторское право в сети Интернет». Количественные: 15 участников. Качественные: разъяснение правил использования контента.

3. Семинар «Создание контента, соответствующий авторскому праву». Количественные: 15 участников. Качественные: создание контента в рамках авторского права.

4. Встреча «Опасности сети Интернет». Количественные: 15 участников. Качественные: обсуждение угроз сети Интернет и способов противодействия им.

5. Встреча «Психологическое воздействие в социальных сетях». Количественные: 15 участников. Качественные: обсуждение психологического воздействия в социальных сетях и способов противодействия им.

6. Комплекс мероприятий по учебно-методическому пособию «Практическая психология безопасности. Управление персональными данными в Интернете»[1]. Количественные: 15 участников. Качественные: обучение, включающее в себя 10 уроков и оценка уровня информационной безопасности молодежи.

Проект не предполагает коммерческий эффект, так как носит социальную направленность, следовательно, расчет периода его окупаемости не требуется.

[1]Солдатова Г.У., Приезжева А.А., Олькина О.И., Шляпников В.Н. Практическая психология безопасности. Управление персональными данными в интернете: учеб.-метод. пособие для работников системы общего образования. М., 2017. С. 88-94.

3.2. Описание мероприятий проекта «Организация комплекса мероприятий по повышению уровня культуры информационной безопасности»

Актуальность: В последнее время современная молодежь не заботится об информационной безопасности в сети Интернет. Это подтверждается социологическим исследованием, результаты которого изложены в 2.1. Тем не менее, можно сделать следующие выводы:

1. Наблюдается заинтересованность молодежью Интернетом. Проведение более 3 часов за компьютером ежедневно у 63% респондентов. Использование компьютера в различных целях, в частности, использование электронной почты, социальных сетей, контента в различных целях. Также молодежь испытывает определенные трудности при выполнении поставленных целей.

2. Кроме того, молодежь использует аккаунты в социальных сетях в различных целях. Именно на ликвидацию информационной неграмотности направлен мой проект.

Цель: Организовать комплекс мероприятий на базе ЦМИ г. Белгород по повышению уровня культуры информационной безопасности для молодежи 14-20 лет до 28.05.18.

Требования к результату: Передача знаний, направленных на повышение культуры информационной безопасности не менее 30 учащимся[1].

Целевая группа: учащиеся города Белгород, 14-20 лет количеством 30 человек.

Место: ЦМИ, г. Белгород.

Мероприятия проводятся с желающими, оцениваются занятия в группе.

Материально-техническое обеспечение предоставляется УМП по Белгородской области.

---

[1]Бочаров М.П., Чумиков А.Н., Самойленко С.А. Реклама и связи с общественностью: профессиональные компетенции. М., 2016. С. 36-40.

Краткое описание сути проекта: Цикл мероприятий представляет собой встречи и семинары по различным направлениям информационной безопасности.

Тип проекта: региональный.

Форма проведения: смешанная.

Задачи:

1. Передача знаний школьников по информационной безопасности;
2. Формирование стремления к творческому процессу познания и выполнению действий по алгоритму.

План мероприятий проекта направлен на повышение уровня культуры информационной безопасности и включает 16 мероприятий.

Визуализация вопросов организации и ресурсного обеспечения внедрения проектных мероприятий представлена на Схеме 2.

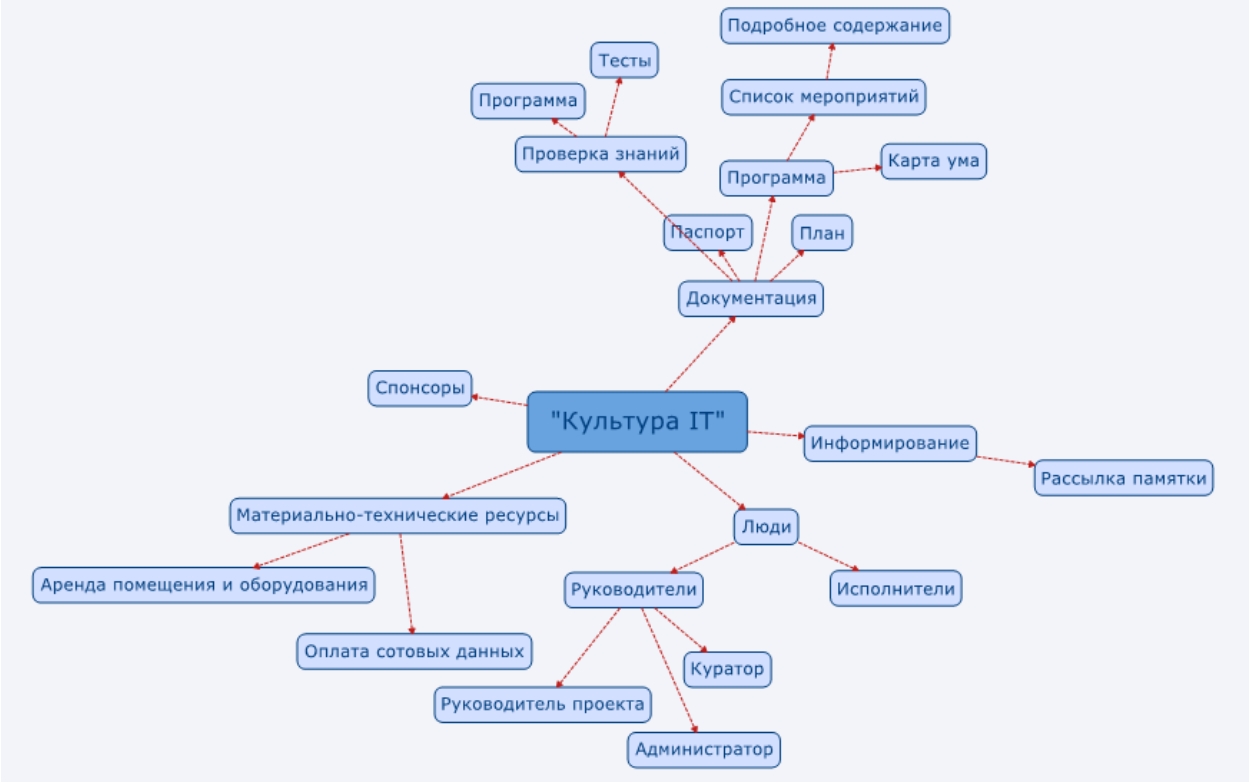

Схема 2. Визуализация вопросов организации и ресурсного обеспечения внедрения проектных мероприятий.

Общий план мероприятий.

1. Определение уровня информационной безопасности молодежи. Социологическое исследование. Количество участников: 154. Место проведения: Белгородская область. Вид подтверждения: результаты анкетирования.

2. Рассылка памятки, посвященной информационной безопасности. Количество участников: 30. Место проведения: г. Белгород. Вид подтверждения: отчет.

3. Мониторинг социальной сети ВКонтакте на предмет противоправного контента («Кибердружина»). Количество участников: 1. Место проведения: г. Белгород. Вид подтверждения: характеристика руководителя практики.

4. Встреча, посвященная авторскому праву в сети Интернет. Количество участников: 15. Место проведения: ЦМИ, г. Белгород. Вид подтверждения: отчет.

Содержание:

1) Объект Авторского права.

2) Субъект Авторского права.

3) Права автора.

4) Охрана смежных прав.

5) Защита авторских и смежных прав.

6) Законы, регулирующие Авторское право.

5. Семинар, посвященный созданию контента в соответствии с авторским правом. Место проведения: ЦМИ, г. Белгород. Вид подтверждения: отчет.

Содержание:

1) Поиск аудио- и фото-продукции, не защищенная Авторским правом.

2) Определение соответствия найденных материалов Авторскому праву

3) Бесплатные программы для создания контента.

6. Встреча, посвященная опасностям сети Интернет. Количество участников: 15. Место проведения: ЦМИ, г. Белгород. Вид подтверждения: отчет.

Содержание:

1) Угрозы сети Интернет.

2) Способы борьбы с угрозами сети Интернет.

3) Программные средства борьбы с угрозами сети Интернет.

7. Встреча, посвященная психологическим воздействиям в сети Интернет. Количество участников: 15. Место проведения: ЦМИ, г. Белгород. Вид подтверждения: отчет.

Содержание:

1) Виды психологического воздействия на пользователя.

2) Способы психологического воздействия на пользователя.

3) Противодействие психологическим воздействиям пользователем.

Цикл мероприятий в рамках учебно-методического пособия «Практическая психология безопасности: управление персональными данными в Интернете»[1].

Количество участников: 15. Место проведения: ЦМИ, г. Белгород. Вид подтверждения: отчет.

Урок № 1. Что такое персональные данные?

Содержание:

1) Разминка «Интернет-викторина»

2) Упражнение «Мой профиль»

3) Что современные подростки знают о персональных данных?

Урок № 2. Какими бывают персональные данные?

Содержание:

1) Разминка «Личное – публичное»

2) Упражнение «Информационный светофор»

[1]Солдатова Г.У., Приезжева А.А., Олькина О.И., Шляпников В.Н. Практическая психология безопасности. Управление персональными данными в интернете: учеб.-метод. пособие для работников системы общего образования. М., 2017. С. 98-104.

3) Упражнение «Детективное бюро»

Урок № 3. Как персональные данные попадают в сеть?

Содержание:

1) Разминка «Великий идентификатор»

2) Упражнение «Цифровой след»

3) Упражнение «Заметаем следы»

Урок № 4. Почему нужно управлять персональными данными?

Содержание:

1) Разминка «По секрету всему свету»

2) Упражнение «Скорая помощь онлайн»

Урок № 5. Как защитить персональные данные?

Содержание:

1) Разминка «Сто к одному»

2) Упражнение «Занимательная криптография»

3) Упражнение «Конкурс социальной рекламы»

4) Как работают хакеры?

Урок № 6. Что такое приватность и личные границы?

Содержание:

1) Разминка «Мои границы»

2) Упражнение «Персональные данные и личные границы»

Урок № 7. Как настраивать приватность в сети?

Содержание:

1) Разминка «Открытость — закрытость»

2) Упражнение «Золотая середина»

3) Упражнение «Моя приватность в сети»

Урок № 8. Как управлять репутацией в сети?

Содержание:

1) Разминка «Испорченный перепост»

2) Упражнение «Деловая репутация»

3) Упражнение «С разных точек зрения...»

4) Лайкни и уволься: как потерять работу из-за активности в социальных сетях

Урок № 9. Что мой смартфон знает обо мне?

Содержание:

1) Разминка «Никто, кроме моего смартфона, не знает, что я...»

2) Упражнение «Умные вещи»

3) Упражнение «Лаборатория мобильных приложений»

4) Защищают ли мессенджеры персональные данные пользователей?

Урок № 10. Как удалить персональные данные из интернета?

Содержание:

1) Разминка «История Марио Гонсалеса»

2) Упражнение «Право на забвение»

Характеристика текущей ситуации и желаемые перспективы развития. Оценивание текущей ситуации будет производиться, по нашему мнению, на основе проведенного социологического исследования (Параграф 2.1.) по трем направлениям: информационная безопасность, правосознание и коммуникация. Градация ответов пользователей представлена по убыванию.

Молодежь активно пользуется Интернетом и социальными сетями, использует аутентификацию и антивирусные средства, резервное копирование. Респонденты оценивают уровень информационной безопасности как «хорошо-удовлетворительно». Основную опасность видят в: 1) мошенниках, хакерах; 2) вредоносных программах; 3) нежелательном содержании; 4) азартных играх; 5) интернет-зависимости; 6) интернет-хулиганах; 7) сексуальных домогательствах; 8) некорректности общения.

Причиной такой ситуации, по результатам социсследования, являются:

1) отсутствие навыка противодействия мошенникам, хакерам;

2) отсутствия навыка планирования времени, однако на вопрос о зависимости сети Интернет на решение других задач большинство опрошенных ответило «нет».

3) Отсутствие контроля со стороны родителей.

4) Не развита культура информационной безопасности.

Текущий уровень информационной безопасности – средний. Так как большинство опрошенных используют различные средства обеспечения информационной безопасности, кроме облачных сервисов. В перспективе желателен высший уровень информационной безопасности.

Молодежь считает, что необходимо правовое регулирование в области информационной безопасности. Большинство опрошенных активно пользуется сетью Интернет в целях потребления контента. Оцениваемый нами уровень: базовый. Мы полагаем, что необходимо освещать молодежи законодательство, в том числе, и в области авторского права (средний уровень).

Причиной этого является ответы респондентов на вопрос о способах повышения культуры информационной безопасности, где ответы были распределены следующим образом: 1) защита персональных данных; 2) разработка нормативно-правового законодательства в сети Интернет; 3) проведение курсов по информационной безопасности; 4) самообразование по информационной безопасности; 5) мониторинг сети Интернет; 6) лицензирование информационной деятельности.

Большинство респондентов пользуются интернетом более трех часов в день. Имеют несколько аккаунтов, среди которых ВКонтакте, Одноклассники, Telegram и Facebook. Тем не менее, приоритетной социальной сетью является ВКонтакте. Большинство используют социальные сети для общения с другими пользователями в различных целях. Респонденты способны устанавливать коммуникационные связи в сети Интернет. Желаемый уровень – договорной, предполагающий обсуждение и согласование с другими участниками интернета на основе предварительных переговоров, а также противодействие психологическому воздействию.

3.3. Условия коммерциализации проекта «Организация комплекса мероприятий по повышению уровня культуры информационной безопасности»

Определим перспективы коммерциализации проекта. Коммерциализацией является деятельность лица или организации, предприятия, направленная на извлечение прибыли всеми способами, это также, если говорить в государственном масштабе, первые шаги при приватизации государственных предприятий, увеличение числа коммерческих предприятий[1].

Для ведения коммерческой деятельности необходимо оформление ИП или юридического лица. Несоблюдение влечет административную ответственность в виде штрафа от 500 до 2000 рублей (ст. 14.1 КоАП РФ). Налоговая ответственность предусмотрена ст. 116 Налогового кодекса РФ влечет взыскание штрафа в размере 10 тысяч рублей. Ведение деятельности влечет взыскание штрафа в размере 10 процентов от доходов, полученных в течение указанного времени в результате такой деятельности, но не менее 40 тысяч рублей. Возможна уголовная ответственность вплоть до лишения свободы на полгода.

Также необходимо получение образовательной лицензии. Однако согласно ФЗ-273 «Об образовании в РФ» не лицензируется следующая деятельность:

- Мастер-классы (заключение договора)
- Разовые ознакомительные семинары
- Вебинары любой тематики
- Обмен опытом
- Конференции, симпозиумы, слеты
- Информационно-консультационные услуги (не обучающие и на возмездной основе)

[1]Коммерциализация – это... URL: https://biznes-prost.ru/kommercializaciya.html (дата обращения: 03.10.2017).

- Развлекательные мероприятия.

Основные характеристики такой деятельности: ознакомление, не предполагает повышение квалификации, возможно получение свидетельства об участии. Образовательно-обучающей деятельностью является овладение знаниями, умениями и навыками, развитие способностей и опыта.

Согласно ПП РФ № 966 лицензия на образовательную деятельность не требуется, если:

- Оказывается, лично предпринимателем, без привлечения других специалистов

- Лекции, семинары, тренинги

Данные услуги считаются культурными или досуговыми. Таким образом, для коммерциализации данного проекта необходимо учреждение ИП или юридического лица. При осуществлении досуговой деятельности необходимо учитывать Закон «Об образовании в РФ» № 273-ФЗ, Закон «О лицензировании» № 99-ФЗ и ПП РФ № 966 при планировании комплекса мероприятий.

Существуют различные способы и схемы реализаций коммерциализации проекта. Поскольку разрабатываемый проект представляет собой комплекс социально направленных мероприятий, коммерциализировать его как продукт не представляется возможным. Однако, для привлечения ресурсов на реализацию проекта есть несколько вариантов.

1. Данные мероприятия могут быть включены в план мероприятий органов управления молодежной политики с бюджетным финансированием.

2. Данные мероприятия могут быть включены в план мероприятий некоммерческой или общественной организации с финансированием из средств грантов.

3. Размещение информации о проекте на краудфандинговой платформе Boomstarter.ru или Planeta.ru для привлечения средств пользователей платформы.

Любой из предложенных вариантов может быть реализован.

На основании третьего раздела можно сделать следующие выводы.

Первое, следует выделить показатели реализации проекта «Организация комплекса мероприятий по повышению уровня культуры информационной безопасности». Их три: оценка текущего уровня информационной безопасности молодежи, поиск противоправного контента в сети Интернет и организация досуговой деятельности по повышению уровня культуры информационной безопасности молодежи. Качественные показатели: количество участников. В первом – 154, во втором – 100 случаев в месяц, в третьем – 15 участников (группа). Качественные показатели: в первом случае – уровень информационной безопасности молодежи, во втором – повышение сознательности пользователей социальной сети ВКонтакте, передача информации о противоправных действиях компетентным органам. В третьем – передача знаний и их оценка. Проект не предполагает коммерческий эффект, так как носит социальную направленность, следовательно, расчет периода его окупаемости не требуется.

Второе, молодежь активно пользуется Интернетом и социальными сетями, использует аутентификацию и антивирусные средства, резервное копирование. Респонденты оценивают уровень информационной безопасности как «хорошо-удовлетворительно». Молодежь считает, что необходимо правовое регулирование в области информационной безопасности. Оцениваемый нами уровень: базовый. Большинство респондентов пользуются интернетом более трех часов в день. Имеют несколько аккаунтов, среди которых ВКонтакте, Одноклассники, Telegram и Facebook. Тем не менее, приоритетной социальной сетью является ВКонтакте. Большинство используют социальные сети для общения с другими пользователями в различных целях. Предположительный текущий уровень – общительный. Респонденты способны устанавливать коммуникационные связи в сети Интернет.

Третье, проект может быть коммерциализирован через несколько вариантов:

1. Включением в план мероприятий органов управления молодежной политики с бюджетным финансированием.

2. Включением в план мероприятий некоммерческой или общественной организации с финансированием из средств грантов.

3. Размещением информации о проекте на краудфандинговой платформе Boomstarter.ru или Planeta.ru для привлечения средств пользователей платформы.

ЗАКЛЮЧЕНИЕ

В России проводятся различные мероприятия в сфере информационной безопасности. Однако сейчас ясно выделились два решения в данной сфере.

Первое решение представляет собой поиск нежелательной информации в Интернете добровольцами и обращение в Роскомнадзор с целью ее блокирования. В этом случае молодежь выступает как активный инструмент воздействия – субъект. На сегодняшний момент времени данное решение оформилось в кибердружины. «Кибердружина» – межрегиональное молодежное общественное движение, которое объединяет более 20 тысяч добровольцев со всей России и стран СНГ, борющихся с преступлениями в виртуальной среде.

Второе решение представляет собой просвещение молодежи в сфере информационных технологий, заключающееся в объяснении ей способов защиты от вредной информации. В этом случае молодежь выступает в качестве объекта воздействия, поглощая предоставляемую учителями, организаторами работы с молодежью информацию. Выделяют следующие направления.

Во-первых, это предоставление покрытия Интернета в регионах. Реализуется это благодаря Ростелекому. Осуществляется это для различных целей, одной из которых является поиск пропавших без вести.

Во-вторых, это образовательная деятельность в рамках учреждений. Например, «Единый урок информационной безопасности в сети Интернет». Также Фонд Развития Интернет с МТС создал «Урок полезного и безопасного Интернета».

В-третьих, образовательная деятельность в сети Интернет. Ведет активную деятельность и Координационный центр доменов RU/.РФ. Проекты для детей и школьников «Изучи Интернет – управляй им!», всероссийский онлайн-чемпионат для школьников (15 тысяч участников). «Позитивный контент» – конкурс сайтов для детей. Также Яндекс реализует

онлайн-проект «Сетевичок». Создана Интернет-среда, содержащая в себе информацию для детей с доменом .ДЕТИ.

В-четвертых, используется технология телефонного и онлайн-консультирования. Фондом Развития Интернет совместно с компаниями МГТС и МТС была запущена линия помощи в 2009 году.

В-пятых, ведется разработка учебно-методической литературы, посвященной безопасности в сети Интернет. Так, Фонд Развития Интернет с МТС В 2013 году разработали методическое пособие «Интернет: возможности, компетенции, безопасность» для работников системы общего образования. В 2016 году совместно с Роскомнадзором было подготовлено пособие «Практическая психология безопасности: управление персональными данными в Интернете» для работников системы общего образования[1].

Ведется работа и на региональном уровне. В Белгородской области также активно развивается направление информационной безопасности молодежи. Так, на сайте Департамента образования Белгородской области активно реализуется проект «Безопасное детство» [2].

На основе проведенного социологического исследования можно сделать вывод о том, что молодежь активно пользуется Интернетом и социальными сетями, использует аутентификацию и антивирусные средства, резервное копирование. Респонденты оценивают уровень информационной безопасности как «хорошо-удовлетворительно». Молодежь считает, что необходимо правовое регулирование в области информационной безопасности. Оцениваемый нами уровень: базовый. Большинство респондентов пользуются интернетом более трех часов в день. Имеют несколько аккаунтов, среди которых ВКонтакте, Одноклассники, Telegram и Facebook. Тем не менее, приоритетной социальной сетью является ВКонтакте. Большинство используют социальные сети для общения с

[1]Единый урок безопасности // Фонд Развития Интернет. 2017. № 26. С. 10-14.

[2]Безопасное детство. URL: https://образование31.рф/our-projects/information-security-of-children-and-adolescents/ (дата обращения: 23.09.2017).

другими пользователями в различных целях. Предположительный текущий уровень – общительный. Респонденты способны устанавливать коммуникационные связи в сети Интернет.

Проектная идея выпускной квалификационной работы представляет собой проведение цикла мероприятий, направленных на повышение уровня культуры информационной безопасности. Данный цикл представляет собой комплекс занятий, включающий в себя лекции с интерактивными элементами, проведение уроков, оценка уровня информационной безопасности молодежи.

Новизна проекта имеет 5 уровень: использование опыта районов и повторение проекта на разных территориях одного региона. Проект не предполагает коммерческий эффект, так как носит социальную направленность, следовательно, расчет периода его окупаемости не требуется.

Таким образом, можно сделать вывод о комплексности взаимодействия в рамках выпускной квалификационной работе: теоретико-методологических основ, социологического исследования и проектной идеи.

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Федеральный Закон «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями) от 27 июля 2006 г. № 149-ФЗ [Текст] – М. : Российская газета, 2006. – 29 июля.

2. Федеральный Закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» (с изменениями и дополнениями) от 9 февраля 2009 г. № 8-ФЗ [Текст] – М. : Российская газета, 2009. – 13 февраля.

3. Федеральный Закон «О персональных данных» от 29 июля 2006 г. № 152-ФЗ [Текст] – М. : Российская газета, 2006. – 29 июля.

4. Федеральный Закон «О средствах массовой информации» от 27 декабря 1991 г. № 2124-1. [Текст] – М. : Российская газета, 2007. – 28 ноября.

5. Указ Президента РФ от 28 июня 1993 г. № 966 «О Концепции правовой информатизации России» (с изменениями и дополнениями) [Текст] // Российская газета. – 1993. – 03 июля.

6. Указ Президента РФ от 01 ноября 2008 г. № 1576 «О Совете при Президенте РФ по развитию информационного общества в РФ» [Текст] // Российская газета. – 2008. – 14 ноября.

7. Об утверждении Основ государственной молодежной политики Российской Федерации на период до 2025 года : Распоряжение Правительства РФ от 29 ноября 2014 г. № 2403-р. [Текст]// СЗ РФ. – 2014. – № 50. – Ст. 7185.

8. Всеобщая декларация прав человека [Электронный ресурс] // Режим доступа к изд. : http://www.consultant.ru/document/cons_doc_LAW_120805/ – Систем. требования: IBM PC, Internet Explorer.

9. Всемирная конвенция об авторском праве [Электронный ресурс] // Режим доступа к изд. : http://docs.cntd.ru/document/1900510 – Систем. требования: IBM PC, Internet Explorer.

10. Всеобщая декларация ЮНЕСКО о культурном разнообразии [Электронный ресурс] // Режим доступа к изд. : http://www.un.org/ru/documents/decl_conv/declarations/cultural_diversity.shtml – Систем. требования: IBM PC, Internet Explorer.

11. Декларация принципов и План действий [Электронный ресурс] // Режим доступа к изд. : http://library.zntu.edu.ua/zakon/03declar.html – Систем. требования: IBM PC, Internet Explorer.

12. Доктрина информационной безопасности РФ [Электронный ресурс] // Режим доступа к изд. : http://www.scrf.gov.ru/documents/5.html – Систем. требования: IBM PC, Internet Explorer.

13. Конвенция об охране нематериального культурного наследия [Электронный ресурс] // Режим доступа к изд. : http://www.un.org/ru/documents/decl_conv/conventions/cultural_heritage_conv – Систем. требования: IBM PC, Internet Explorer.

14. Окинавская Хартия глобального информационного общества [Электронный ресурс] // Режим доступа к изд. : http://www.kremlin.ru/supplement/3170 – Систем. требования: IBM PC, Internet Explorer.

15. Проект Концепции стратегии кибербезопасности Российской Федерации [Электронный ресурс] // Режим доступа к изд. : http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf. – Систем. требования: IBM PC, Internet Explorer.

16. Тунисская программа для информационного общества [Электронный ресурс] // Режим доступа к изд. : http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/bc05d17935b393aac32575a8004cd760 – Систем. требования: IBM PC, Internet Explorer.

17. Хартия о сохранении цифрового наследия [Электронный ресурс] // Режим доступа к изд. : http://www.ifap.ru/ofdocs/unesco/digit.htm – Систем. требования: IBM PC, Internet Explorer.

18. Абрамов, Ю.Ф. Информационная цивилизация: природа и перспективы развития [Текст] / Ю.Ф. Абрамов, О.В. Бондаренко, В.К. Душутин. – Иркутск : Редакционно-издательский отдел Иркутского государственного университета, 1998. – 97 с.

19. Антопольский, А.А. Ответственность за правонарушения при работе с конфиденциальной информацией [Текст] / А.А. Антопольский // Административная ответственность. – 2001. – № 2. – С. 124-130.

20. Апресян, Р.Г. Идея морали и базовые нормативно-этические программы [Текст] /Р.Г. Апресян – М.: Институт философии, 1995. – 353 с.

21. Асаул, А.Н. Организация предпринимательской деятельности [Текст] / А.Н. Асаул. – Санкт-Петербург : АНО ИПЭВ, 2009. – 336 с.

22. Бакштановский, В.И. Честная игра: Нравственная философия и этика предпринимательства [Текст] / В.И.Бакштановский, Ю.В. Согомонов. – Томск: Томск.ун-т, 1992. – 240 с.

23. Бачило, И.Л. Информационное право: основы практической информатики [Текст] / И.Л. Бачило. – М. : Юринформцентр, 2001. – 352 с.

24. Бородакий, Ю. В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века [Текст] / Ю.В. Бородакий, А.Ю. Добродеев, И.В. Бутусов // Вопросы кибербезопасности. – 2013. – № 1. – С. 27-30.

25. Бочаров, М. П. Реклама и связи с общественностью: профессиональные компетенции [Текст] / М.П. Бочаров, А.Н. Чумиков, С.А. Самойленко. – М. : РАНХиГС, 2016. – 110 с.

26. Белл, Д. Грядущее постиндустриальное общество [Текст] / Д. Белл. – Москва: Academia, 1999. – 124 с.

27. Васенин, В.А. Ингформационная безопасность и компьютерный терроризм [Текст] / В.А. Васенин // Научные и методологические проблемы информационной безопасности. – 2004. – № 10. – С. 67-85.

28. Ващекин, Н.П. Безопасность и устойчивое развитие России [Текст] / Н.П. Ващекин, М.И. Дэлиев, А.Д. Урсул. – М. : МГУК, 1998. – 446 с.

29. Винер, Н. Кибернетика, или управление и связь в животном и машине [Текст] / Н. Винер. – М.: Советское радио, 1958. – 215 с.

30. Возженников, А.В. Основные концептуальные положения безопасности России в XXI веке [Текст] / А.В. Возженников, И.Н. Глебов, В.А. Золотарев. – М.: ЭДАСПАК, 2000. – 48 с.

31. Войскунский, А.Е. Информационная безопасность: психологические аспекты [Текст] /А.Е. Войскунский // Национальный психологический журнал. – 2010. – № 1(3). – С. 48-53.

32. Галинская, И.Л. Этико-правовое пространство информационно-компьютерных технологий [Текст] / И.Л. Галинская, А.И. Панченко // Новые инфокоммуникационные технологии в социально-гуманитарных науках и образовании: современное состояние, проблемы, перспективы развития. – 2003. – № 2. – С. 112-132.

33. Гендина, Н.И. Формирование информационной культуры личности в библиотеках и образовательных учреждениях : учеб.-метод. пособие [Электронный ресурс] / Н. И. Гендина // Режим доступа к изд. : http://www.mediagram.ru – Систем. требования: IBM PC, Internet Explorer.

34. Грачев, Г.В. Информационно-психологическая безопасность личности: теория и технология психологической защиты: автореф. дис. ... д-ра психол. наук [Текст] / Г.В. Грачев. – М.: МГУ, 2000. – 18 с.

35. Гриняев, С.Н. Интеллектуальное противодействие информационному оружию [Текст] / С.Н. Гриняев. – М.: Синтег, 1999. – 232 с.

36. Гриняев, С.Н. Поле битвы – киберпространство: теория, приемы, средства, методы и системы ведения информационной войны [Текст] / С.Н. Гриняев. – Минск, 2004. – 448 с.

37. Гусейнов, А.А. Золотое правило нравственности [Текст] / А.А. Гусейнов. – М.: Молодая гвардия, 1988. – 271 с.

38. Дайзард, У. Наступление информационного века. Новая технократическая волна на Западе [Текст] / У.Дайзард. – М.: Мысль, 1986. – 412 с.

39. Дзлиев, М.И. Проблемы безопасности: теоретико-методологические аспекты [Текст] / М.И. Дзлиев, А.Л. Романович, А.Д. Урсул. – М.: МГУК, 2001. – 192 с.

40. Емельянов, Г.В. Проблемы обеспечения информационно-психологической безопасности России [Текст] / Г.В. Емельянов, В.Е. Лепский, А.А. Стрельцов // Информационное общество. – 1999. – № 3. – С. 47-51.

41. Ермаков, Ю.А. Манипуляция личностью: смысл, приёмы, последствия [Текст] / Ю.А. Ермаков. – Екатеринбург : Изд-во Уральского ун-та, 1999. – 203 с.

42. Зегжда, П.Д. Теория и практика обеспечения информационной безопасности [Текст] / П.Д. Зегжда, Д.П. Зегжда, П.В. Семьянов, С.В. Семьянов, С.С. Корт, В.М. Кузьмич, И.Д. Медведовский, А.М. Ивашко, А.П. Баранов. – М.: Яхтсмен, 1996. – 298 с.

43. Капурро, Р. Информационная этика [Текст] / Р. Капурро // Информационное общество. – 2010. – №. 5. – С. 5-15.

44. Кастельс, М. Информационная эпоха: экономика, общество и культура [Текст] / М. Кастельс. – М.: АСТ, 2000. – 117 с.

45. Колин, К.К. Информационная культура и качество жизни в информационном обществе [Текст] / К.К. Колин // Открытое образование. – 2010. – № 1. – С. 15-18.

46. Лазарев, И.А. Информационная безопасность [Текст] / И.А. Лазарев. – М.: МГЦНТИ, 1997. – 336 с.

47. Лопатин, В.Н. Безопасность – информационный выбор России в XXI в. [Текст] / В.Н. Лопатин. – М.: Космосинформ, 2003. – 194 с.

48. Малюк, А.А. Введение в защиту информации в автоматизированных системах [Текст] / А.А. Малюк, С.В. Пазизин, Н.С. Погожин. – М.: Горячая линия – Телеком, 2001. – 148 с.

49. Малюк, А.А. Гуманитарные аспекты информационной безопасности, образование, система подготовки специалистов в области информационной безопасности [Текст] / А.А.Малюк, О.Ю. Полянская // Вестник РГНФ. – 2011. – № 4(65). – С. 72-78.

50. Манжуева, О.М. Феномен информационной безопасности: сущность и особенности: автореф. дис. ... д-ра филос. наук [Текст] / О.М.Манжуева; Бурятский государственный университет. – Улан-Удэ, 2015. – 45с.

51. Манойло, А.В. Государственная информационная политика в особых условиях [Текст] / А.В. Манойло. – М.: МИФИ, 2003. – 388 с.

52. Мельник, И.К. Манипулирование личностью: организация, способы и технологии информационно-психологического воздействия [Текст] / И.К. Мельник, Г.В. Грачев. – М.: Эксмо, 2002. – 112 с.

53. Мелюхин, И. С. Информационное общество: истоки, проблемы, тенденции развития [Текст] / И.С.Мелюхин. – М.: Издательство МГУ, 1999. – 201 с.

54. Назаретян, А.П. Агрессия, мораль и кризисы в развитии мировой культуры [Текст] / А.П. Назаретян. – М.: Наследие, 1996. – 183 с.

55. Назаров, В.Н. Прикладная этика [Текст] / В.Н. Назаров. – М.: Гардарики, 2005. – 320 с.

56. Панарин, А.С. Стратегическая нестабильность в XXI веке [Текст] / А.С. Панарин. – М.: Алгоритм, 2003. – 560 с.

57. Петров, В.П. Информационная безопасность человека и общества [Текст] / В.П. Петров, С.В. Петров. – М.: ЭНАС, 2007. – 304 с.

58. Плешаков, В.А. Киберсоциализация человека: от Homo Sapiens'а до Homo Cyberus'а [Текст] / В.А.Плешаков. – М.: Прометей, 2011. – 119 с.

59. Поздняков, А. И. Информационная безопасность страны и Вооруженных Сил [Текст] / А. И. Поздняков // Национальная безопасность: актуальные проблемы. – 1999. – № 3. – С. 171-173.

60. Попов, В.Д. Парадигмы исследования информационных процессов [Текст] / В.Д. Попов. – М.: РАГС, 2010. – 60 с.

61. Почепцов, Г.Г. Информационно-психологическая война [Текст] / Г.Г. Почепцов. – М.: СИНТЕГ, 2000. – 180 с.

62. Ракитов, А.И. Информационная революция как фактор экономического и социального развития [Текст] / А.И. Ракитов // Информационная революция: наука, экономика, технология. – 1992. – № 5. – С. 5-17.

63. Расторгуев, С.П. Информационная война. Проблемы и модели. Экзистенциальная математика [Текст] / С.П. Расторгуев. – М.: Гелиос АРВ, 2006. – 240 с.

64. Робертсон, Д.С. Информационная революция [Текст] / Д.С. Робертсон // Информационная революция: наука, экономика, технология – 1992. – № 5. – С. 17-27.

65. Смолян, Г.Л. Сетевые информационные технологии и проблемы безопасности личности [Текст] / Г.Л. Смолян // Информационное общество – 1999. – № 1. – С. 3-8.

66. Старовойтов, А.В. Информационное обеспечение государственного управления [Текст] / В.А. Никитов, Е.И. Орлов, А.В. Старовойтов, Г.И. Савин. – М.: Славянский диалог, 2000. – 415 с.

67. Стерледева, Т. Д. Виртуальная агрессия – следствие взаимодействия человека с электронно-виртуальной реальностью как предметом повышенной опасности [Текст] / Т. Д. Стерледева //

Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. – 2011.– № 8 (14). – С. 181-184.

68. Сычев, М.П. Киберпреступность и подготовка специалистов по борьбе с ней в России [Текст] / Н.В. Медведев, М.П. Сычев, И.Б. Федоров // Информационные технологии. – 2005. – № 9. – С. 2-7.

69. Тонконогов, А.В. Информационно-психологическая безопасность в системе духовной безопасности современной России [Текст] / А.В. Тонконогов, // Власть. – 2010. – № 6. – С. 53-56.

70. Тоффлер, Э. Третья волна [Текст] / Э.Тоффлер. – Москва: АСТ, 1999. – 136 с.

71. Туоминен, С. Педагогические аспекты формирования медийной и информационной грамотности [Текст] / С. Туоминен, С. Котилайнен. – М.: Институт ЮНЕСКО по информационным технологиям в образовании, 2012. – 142 с.

72. Урсул, А.Д. Природа информации (Философский очерк) [Текст] / А.Д. Урсул. – М.: Политиздат, 1968. – 288 с.

73. Уэбстер, Ф. Теории информационного общества [Текст] / Ф. Уэбстер. – М.: Аспект Пресс, 2004. – 400 с.

74. Фатьянов, А.А. Информация как объект права [Текст] / А.А. Фатьянов // Информационная безопасность России в условиях глобального информационного общества. – 2001. – С. 47-52.

75. Цыганков, В.Д. Психотроника и безопасность России [Текст] / В.Д. Цыганков. – М. : Синтег, 2003. – 136 с.

76. Черешкин, Д.С. Нелегкая судьба российской информатизации [Текст] / Д.С. Черешкин, Г.Л. Смолян // Информационное общество. – 2008. – № 1-2. – С. 47-71.

77. Шурухнов, Н.Г. Расследование неправомерного доступа к компьютерной информации [Текст] / Ю.В. Гаврилин, А.В. Пушкин, Е.А. Соцков, Н.Г. Шурухнов. – М.: Щит-М, 1999. – 254 с.

78. Ясенев, В.Н. Информационная безопасность в экономических системах [Текст] / В.Н. Ясенев. – Н. Новгород: ННГУ, 2006. – 253 с.

79. Урсул, А.Д. Природа информации (Философский очерк) [Текст] / А.Д. Урсул. – М.: Политиздат, 1968. – 608 с.

80. Информационное общество в Российской Федерации. 2017 [Текст]: Стат. сб. / Росстат. – М., 2017.

81. Медиа- и информационная грамотность в обществе [Текст] : материалы междун. конф. г. Москва, 19-20 апреля 2013 г. / под общ. ред. М.К. Торрас-Кальво. – М.: МЦБС, 2013. – 235 с.

82. Безопасное детство [Электронный ресурс] // Режим доступа к изд. : https://образование31.рф/our-projects/information-security-of-children-and-adolescents/ – Систем. требования: IBM PC, Internet Explorer.

83. Безопасность персональных данных [Электронный ресурс] // Режим доступа к изд. : https://www.levada.ru/2017/05/25/bezopasnost-personalnyh-dannyh/ – Систем. требования: IBM PC, Internet Explorer.

84. ВЦИОМ-Спутник [Электронный ресурс] // Режим доступа к изд. : https://wciom.ru/index.php?id=236&uid=116691 – Систем. требования: IBM PC, Internet Explorer.

85. Информационная безопасность [Электронный ресурс] // Режим доступа к изд. : http://hotmijskou.net/elektron_servise/Telefoni.htm – Систем. требования: IBM PC, Internet Explorer.

86. Кибердружина [Электронный ресурс] // Режим доступа к изд. : http://www.ligainternet.ru/liga/activity-cyber.php – Систем. требования: IBM PC, Internet Explorer.

87. Кибердружина. Старый Оскол [Электронный ресурс] // Режим доступа к изд. : https://vk.com/kiberdruzhin.oskol – Систем. требования: IBM PC, Internet Explorer.

88. «Национальная программа поддержки и развития чтения», разработанная Федеральным агентством по печати и массовым коммуникациям совместно с Российским книжным союзом [Электронный

ресурс] // Режим доступа к изд. : http://www.library.ru/1/act/doc.php?o_sec=130&o_doc=1122 – Систем. требования: IBM PC, Internet Explorer.

89. Стратегический план программы ЮНЕСКО «Информация для всех» на 2008-2013 гг. [Электронный ресурс] // Режим доступа к изд. : http://www.ifap.ru/ofdocs/unesco/sp813.pdf – Систем. требования: IBM PC, Internet Explorer.

90. Татарстанскую молодёжь защитят от интернета [Электронный ресурс] // Режим доступа к изд. : https://www.idelreal.org/a/28664674.html – Систем. требования: IBM PC, Internet Explorer.

91. Форум по вопросам управления Интернетом (ФУИ). Третье совещание. Обобщающий документ [Электронный ресурс] // Режим доступа к изд. : http://www.ifap.ru/pr/2008/n081201a.pdf – Систем. требования: IBM PC, Internet Explorer.

92. Masuda Y. The information society as post-industrial society. – Washington: World Future Society, 1983.

ПРИЛОЖЕНИЯ

Приложение 1

Программа социологического исследования «Определение уровня информационной безопасности молодежи»

Обоснование проблемы исследования. Информатизация, развитие научно-технической революции, использование новых систем управления, непрерывное обучение персонала послужила переходу в постиндустриальное общество. Все это послужило активному развитию глобальности развития информационных технологий, в частности, Интернета, электронной почты, цифрового телевидения и ряда других средств.

Молодежь – самая подверженная влиянию группа населения. Это обусловлено возрастными особенностями: сперва физиологическими особенностями (половое созревание; быстрый рост конечностей, который приводит к скачкам артериального давления), а затем и к психологическим (общению, максимализму, тяге к новому). Информационные технологии, используемые в современном обществе, оказывают огромное влияние на глобальное развитие. Постоянное развитие данной области несет изменения в увеличении скорости и объемов передачи информации, новых способах общения. Немаловажную роль играет и сеть Интернет.

Она стала местом распространения различного вида угроз против охраняемых законом важнейших интересов социума. Все выше перечисленное ставит перед обществом новую проблему – определение уровня культуры информационной безопасности молодежи.

Степень научной разработанности. Технологиям обеспечения информационной безопасности посвящены работы В.А. Васенина, Д.П. Зегжды, А.А. Малюка, Е.И. Орлова, А.В. Старовойтова, М.П. Сычева, Н.Г. Шурухнова, В.Н. Ясенева и др. Авторы рассматривают технические приемы и методы обеспечения защиты компьютерной информации и информационных систем.

Междисциплинарная проблематика информационной безопасности является предметом исследований А.Н. Асаула, А.В. Возженникова, И.А. Лазарева, А.И. Позднякова и др., синтезировать гуманитарную и техническую составляющие информационной безопасности пытаются Г.Г. Почепцов, С.П. Расторгуев и др., социологические и политологические аспекты проблемы раскрываются в работах Г.Л. Смоляна, Д.С. Черешкина.

Различные аспекты защиты личности от негативного информационного воздействия раскрывают труды Ю.А. Ермакова, И.Н. Панарина, а также других авторов. В этом ключе выделяется психологическое направление в исследованиях Г.В. Грачева, В.Н. Лопатина, И.К. Мельника, В.Д. Цыганкова, вопросам правовой защиты интересов личности, общества и государства посвящены работы А.А. Антопольского, И.Л. Бачило, В.Д. Попова, А.А. Фатьянова и т.д.

Концептуальное понимание безопасности в социологии и философии исследуется в работах Н.П. Ващекина, М.И. Дзлиева, А.Д. Урсула и др. Существенный вклад в изучение проблем развития и применения информационных технологий в информационном обществе вносят труды Ю.Ф. Абрамова, С.Н. Гриняева, Г.В. Емельянова, К.К. Колина, А.Н. Кочергина, Н.Н. Моисеева, А.И. Ракитова, Г.Л. Смоляна и др., а также Ж. Бодрийяра, М. Вебера, У. Дайзарда, П. Друкера и др., посвященные социально-философскому анализу информационных технологий как доминанте развития современного общества.

Нами был проведен поиск и анализ статистического показателя[1]. Исследование, проведенное Левада-Центром, было посвящено безопасности персональных данных от 25.05.2017. Опрос проведен 7 – 10 апреля 2017 года по репрезентативной всероссийской выборке городского и сельского населения среди 1600 человек в возрасте 18 лет и старше в 137 населенных пунктах 48 регионов страны. Исследование проводилось на дому

[1]Безопасность персональных данных. URL: https://www.levada.ru/2017/05/25/bezopasnost-personalnyh-dannyh/ (дата обращения: 23.09.2017).

у респондента методом личного интервью. Распределение ответов приводится в процентах от общего числа опрошенных вместе с данными предыдущих опросов.

Рисунок 1. Вопрос «Информированы ли Вы о возможном получении личных данных пользователя хакерами при использовании мобильным телефоном и Интернетом?»

На вопрос об информированности населения о возможном получении личных данных пользователя хакерами при использовании мобильным телефоном и Интернетом в сравнении между январем 2012 года и апрелем 2017 года, число осведомленных выросло, количество не осведомленных снизилось. Общая же обеспокоенность касательно этого вопроса возросла (Рисунок 1). Количество пользователей, предпринимающих различные способы защиты личной информации выросло, а бездействующих снизилось.

На вопрос о причинах бездействия защиты персональной информации в динамике январь 2012 – апрель 2017, несколько выросло число респондентов, не видящих смысла в защите персональной информации.

Рисунок 2. Вопрос «Назовите причины бездействия защиты персональной информации»

Количество воздержавшихся также несколько выросло (Рисунок 2).

На вопрос о необходимости деанонимизации в социальных сетях в динамике за январь 2012, март 2014 и апрель 2017 количество согласных увеличилось примерно вдвое, количество несогласных несколько снизилось. Число неопределившихся также снизилось (Рисунок 3).

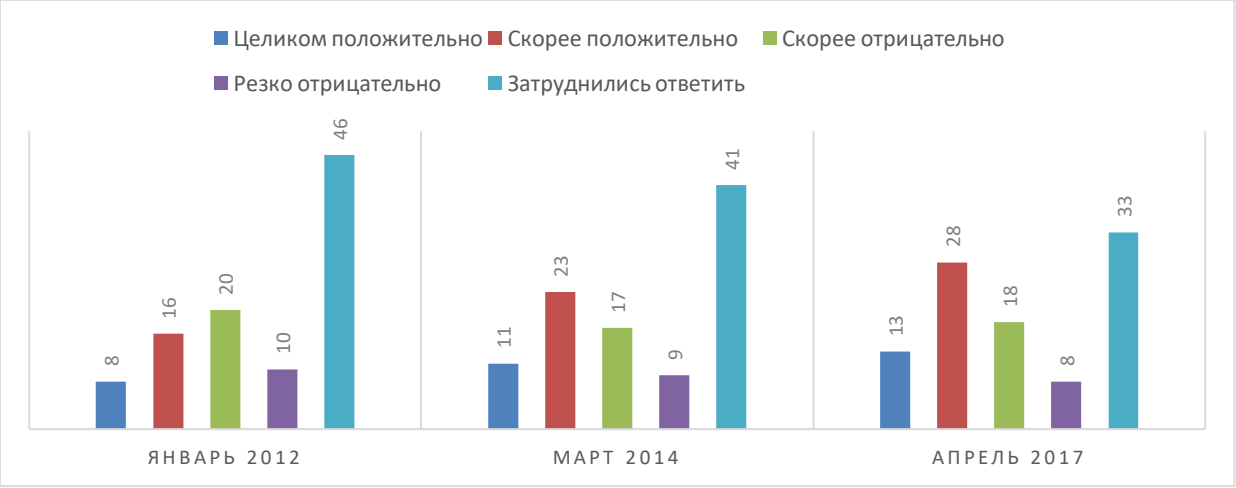

Рисунок 3. Вопрос «Необходима ли деанонимизация в социальных сетях?»

Таким образом, на основе данного исследования можно сделать вывод о том, что число заинтересованных респондентов в повышении информационной безопасности выросло, а количество безучастных граждан

снизилось. Тем не менее, необходимо провести региональное исследование, призванное определить уровень информационной безопасности молодежи.

Проблема социологического исследования заключается в противоречии между возросшими требованиями общества к уровню информационной безопасности молодежи и недостаточной эмпирической разработанностью данной темы.

Объектом социологического исследования выступают студенты и школьники (15-21 лет) Белгородской области, эксперты (специалисты УМП по Белгородской области).

Предметом социологического исследования выступает уровень информационной безопасности молодежи.

Целью социологического исследования выступает изучение уровня информационной безопасности молодежи Белгородской области.

Задачи социологического исследования.

1. Составить программу социологического исследования для выявления уровня информационной безопасности молодежи Белгородской области.
2. Провести пилотажное исследование для выявления уровня информационной безопасности молодежи.
3. Составить программу и провести экспертное исследование для выявления мнения экспертов касательно уровня информационной безопасности молодежи Белгородской области.
4. Систематизировать и интерпретировать полученные материалы, обобщить теоретические и практические результаты исследования, сформулировать выводы и рекомендации, полученные в ходе исследования.

Интерпретация основных понятий.

Информационная безопасность – это комплекс знаний и умений применять их на практике, направленные на обеспечение целостности данных и конфиденциальности информации в сочетании с ее доступностью для всех авторизованных пользователей.

Интернет-портал – это система, предоставляющая информацию, а также ссылки на сторонние ресурсы и сайты всемирной сети Интернет.

Культура информационной безопасности – это определенный уровень развития человека, проявляемый в информационной сфере.

Уровень – качественная характеристика, характеризующая отношение изученности чего-либо.

Отношение – субъективное понимание и знание молодежи информации, касательно информационной безопасности.

Ценность – это значимость объекта окружающей действительности для человека, социальной группы.

Правосознание – это совокупность взглядов объекта исследования на право в рамках информационной безопасности.

Самоорганизация – это способность индивида планировать и достигать цели плана в рамках взаимодействия с информационным полем.

Информированность – владение знаниями, актуальными в настоящее время, а также навыками, необходимыми для получения и анализа этих знаний.

Творчество – это знание и пользование индивидом ресурсов сети Интернет и способностью их использовать для создания какого-либо продукта и/или услуги.

ПО – программное обеспечение – комплекс программ: обеспечивающих обработку или передачу данных; предназначенных для многократного использования и применения разными пользователями[1].

Аутентификация – процедура проверки пользователя[2]. Она необходима для доступа к защищенной пользователем информации.

Социальная зависимость – это комплекс параметров, учитывающие взаимодействие пользователя с **социальными сетями** – сайтам,

---

[1]Программное обеспечение – это... URL: https://dic.academic.ru/dic.nsf/fin_enc/27841 (дата обращения: 03.10.2017).

[2]Аутентификация – это... URL: https://dic.academic.ru/dic.nsf/ruwiki/617128 (дата обращения: 03.10.2017).

предназначенным для обмена информацией, которую добавляют сами пользователи; **мессенджерами** – программами для мгновенного обмена сообщениями между пользователями.

Аккаунт – учетная запись пользователя, позволяющая ему пользоваться социальной зависимостью.

Молодежь – это социально-демографическая группа, выделяемая на основе возрастных особенностей, социального положения и характеризующаяся специфическими интересами и ценностями. Эта группа включает лица в возрасте от 14 до 30 лет, а в некоторых случаях,...–до 35 и более лет, имеющих постоянное место жительства в Российской Федерации или проживающих за рубежом (граждане Российской Федерации и соотечественники)[1].

Контент – любое информационное наполнение ресурса (к примеру, веб-сайта) – вся информация, которую пользователь сможет загрузить на диск компьютера, соблюдая соответствующие законности, как правило, для личного пользования.

Повышение культуры информационной безопасности – это комплекс мероприятий различного характера, направленный на молодежь, включающий поиск угроз информационной безопасности, определение причин их возникновения и выработка средств повышения культуры информационной безопасности молодежи.

Операционализация основных понятий.

Таблица 1

Основное понятие	**Понятие-индикатор**	**Вопрос-индикатор**
Правосознание	1. Определение необходимости правового регулирования в сфере информационной безопасности.	1. Необходимо ли правовое регулирование в сфере информационной безопасности? (Вопрос №2)

[1]Об утверждении Основ государственной молодежной политики Российской Федерации на период до 2025 года: Распоряжение Правительства РФ от 29 ноября 2014 г. № 2403-р. // СЗ РФ. 2014. № 50. Ст. 7185.

Информационная безопасность	1. Что респондент понимает под информационной безопасностью? 2. Определение необходимости организации информационной безопасности через установку и использования программного обеспечения. 3. Определение необходимости респондентом обновления ПО. 4. Использование процедуры аутентификации при использовании собственных устройств. 5. Способы использования респондентом процедуры аутентификации собственных устройств. 6. Самооценка респондента уровня информационной безопасности.	1. Что Вы понимаете под информационной безопасностью? (Вопрос №1) 2. Какие средства для организации информационной безопасности Вы используете? (Вопрос №3) 3. Обновляете ли Вы программное обеспечение? (Вопрос №4) 4. Используете ли Вы процедуру аутентификации при использовании собственных устройств? (Вопрос №5) 5. Выберите из списка способы аутентификации, которыми Вы пользуетесь при использовании собственного устройства. (Вопрос №6) 6. Как Вы сами оцениваете уровень информационной безопасности? (Вопрос №19)
Социальная зависимость	1. Наличие у респондента страницы в социальной сети (мессенджере). 2. Частота использования страницы в социальной сети (мессенджере). 3. Определение названий социальных сетей (мессенджеров), где у респондента есть аккаунт. 4. Определения названия социальной сети (мессенджера) респондента, используемой чаще всего. 5. Характер использования страницы в социальной сети (мессенджере).	1. Имеете ли Вы аккаунт/ы в социальных сетях (мессенджерах)? (Вопрос №7) 2. Как часто Вы пользуетесь социальными сетями (мессенджерами)? (Вопрос №8) 3. Выберите название той социальной сети (мессенджера), где у Вас есть аккаунт/ы. (Вопрос №9) 4. Какую социальную сеть (мессенджер) Вы используете чаще всего? (Вопрос №10) 5. С какой целью Вы используете социальную сеть (мессенджер)? Выберите из списка. (Вопрос №11)
Самоорганизация	1. Определение времени	1. Сколько времени в день

	использования сети Интернет в день. 2. Выявление круга задач, решаемые пользователем при использовании Интернета. 3. Определение влияния Интернета на респондента при выполнении задач, не связанных с Интернетом. 4. Выявление часто используемых устройств, через которые респондент пользуется Интернетом.	Вы проводите, используя Интернет? (Вопрос №12) 2. Какие задачи Вы решаете при использовании Интернета? Выберите из списка. (Вопрос №13) 3. Является ли для Вас Интернет помехой при выполнении других задач, не связанных с Интернетом. (Вопрос №14) 4. Какое устройство Вы используете для выхода в сеть Интернет? (Вопрос №15)
Информированность	1. Способы проверки респондентом достоверности информации в сети Интернет.	1. Каким образом Вы проверяете достоверность информации в сети Интернет? (Вопрос №16)
Творчество	1. Определение круга использования образовательных интернет-порталов респондентом. 2. Определение круга использования информационных интернет-порталов респондентом.	1. Какие образовательные интернет-порталы Вы используете? (Вопрос №17) 2. Какие информационные интернет-порталы Вы используете? (Вопрос №18)
Повышение культуры информационной безопасности	1.Определение актуальных угроз информационной безопасности молодежи. 2. Определение причин подверженности молодежи угрозам в сфере информационной безопасности. 3. Определение путей повышения культуры информационной безопасности молодежи.	1. Какие угрозы в сфере информационной безопасности наиболее актуальны для молодежи? (Вопрос №20) 2. Почему молодежь подвержена угрозам в сфере информационной безопасности? (Вопрос №21) 3. Каким образом необходимо повышать культуру информационной безопасности молодежи? (Вопрос №22)

Гипотезы исследования:

1. Учащаяся молодежь активно (более 3 часов в день) пользуется компьютером.

2. Учащаяся молодежь использует компьютер в основном в досуговых целях.

3. Учащаяся молодежь не проверяет достоверность информации из сети Интернет.

Определение выборочной совокупности.

В данном социологическом исследовании применяется метод серийной (гнездовой) выборки. Здесь предполагается отбор в качестве единиц исследования не отдельных респондентов, а групп (гнезд) с последующим сплошным опросом в отобранных группах. Гнездовая выборка репрезентативна в том случае, если состав групп в максимальной степени схож по основным демографическим признакам респондентов. Поэтому отбор «гнезд» производится по принципу их типичности.

Данное исследование используется как предварительный этап для сбора приблизительных данных об объекте. Изучение необходимо для того, чтобы в дальнейшем провести глубинное исследование. В этой связи, выборочную совокупность будут составлять 154 респондента и 10 экспертов.

Выборочную совокупность данного исследования образует молодежь Белгородской области.

Методы сбора и обработки информации.

В данной программе социологического исследования основным методом сбора первичной социологической информации является метод анкетного опроса, поскольку он позволяет в достаточно короткие сроки выяснить мнение больших совокупностей людей, обработать большое количество первичной информации и получить значительную информацию по рассматриваемой проблеме.

Анкетный опрос – один из двух (второй – анкетирование) основных видов опросных методов, применяемый для получения эмпирической информации, касающейся объективных фактов, знаний, мнений, оценок, поведения. Существенной особенностью анкетного опроса является опосредованный характер взаимодействия между исследователем и

респондентом, которые общаются при помощи анкеты, причем респондент сам читает предлагаемые ему вопросы и сам фиксирует свои ответы.

Респонденты – лица, принимающие участие в социологическом опросе или анкетировании. Они являются объектом исследования.

К достоинствам анкетного опроса относятся:

1) сравнительная экономичность;
2) возможность охвата больших групп людей;
3) применимость к самым различным сторонам жизни людей;
4) хорошая формализуемость результатов;
5) минимум влияния исследователя на опрашиваемого;
6) оперативность;
7) экономия средств и времени.

В данном социологическом исследовании предусмотрен автоматический метод обработки полученной информации с помощью программы Google Forms.

Инструментарий исследования включает в себя анкету.

Анкета – методическое средство для получения первичной социологической информации, оформляемое в виде набора вопросов, логически связанных с центральной задачей и гипотезой исследования (см. Приложение 2).

Всего в анкете молодежи будет задано 26 вопроса по данной теме. Включаемые в анкету вопросы классифицируются по степени стандартизации и делятся на закрытые (11), полузакрытые (14) и открытые (1).

Приложение 2

Анкета социологического исследования «Определение уровня информационной безопасности молодежи»

Анкета

Уважаемый респондент! Вам предложена для заполнения анкета для социологического исследования на тему «Определение уровня информационной безопасности молодежи». Прошу Вас честно ответить на вопросы. Вся полученная от Вас информация останется строго конфиденциальной и будет использована в обобщенном виде. Ваше мнение очень важно для нас!

Инструкция по заполнению вопросов в анкете:

1. В вопросах с открытым ответом, внимательно прочитайте вопрос и напишите свое мнение по нему.

2. В вопросах с предложенными вариантами выберите один или несколько вариантов (отмечено*) (в Google Forms будет соответствующий селектор), который/ые подходит/ят именно Вам.

1. Что Вы понимаете под информационной безопасностью?*

a) Обеспечение конфиденциальности информации
b) Организация доступности информации для авторизованных пользователей
c) Знания и умения, обеспечивающие регулирование информации
d) Затрудняюсь ответить
e) Другое_____

2. Необходимо ли правовое регулирование в сфере информационной безопасности?

a) Да
b) Нет
c) Затрудняюсь ответить

3. Какие средства для организации информационной безопасности Вы используете?*

a) Антивирусные средства
b) Межсетевые экраны
c) Криптографические средства
d) Резервное копирование
e) Системы бесперебойного питания
f) Не пользуюсь средствами для организации информационной безопасности. Переходите к вопросу № 5
g) Другое_____
h) Затрудняюсь ответить

4. Обновляете ли Вы программное обеспечение?

a) Да, автообновление, не получаю уведомления
b) Да, автообновление, получаю уведомления
c) Да, вручную
d) Нет

5. Используете ли Вы процедуру аутентификации при использовании собственных устройств?

a) Да
b) Нет. Переходите к вопросу № 7
c) Затрудняюсь ответить

6. Выберите из списка способы аутентификации, которыми Вы пользуетесь при использовании собственного устройства.*

a) Код-пароль
b) Код-графический ключ
c) Отпечаток пальца
d) Сетчатка глаза
e) Дополнительный код (двухфакторная аутентификация)
f) Другое_____

7. Имеете ли Вы аккаунт/ы в социальных сетях (мессенджерах)?

a) Да, один
b) Да, несколько
c) Нет. Переходите к вопросу № 12

8. Как часто Вы пользуетесь социальными сетями (мессенджерами)?

a) Несколько раз в день
b) Один раз в день
c) Один раз в 3 дня
d) Один раз в неделю
e) Еще реже

9. Выберите название той социальной сети (мессенджера), где у Вас есть аккаунт/ы.*

a) ВКонтакте
b) Одноклассники
c) ДругВокруг
d) Facebook
e) Twitter
f) Telegram
g) Другое_____

10. Какую социальную сеть (мессенджер) Вы используете чаще всего?

a) ВКонтакте
b) Одноклассники
c) ДругВокруг
d) Facebook
e) Twitter
f) Telegram
g) Другое_____

11. С какой целью Вы используете социальную сеть (мессенджер)? Выберите из списка.*

a) Общение с досуговыми целями
b) Общение по работе/учебе
c) Потребление контента в досуговых целях
d) Другое_____

12. Сколько времени в день Вы проводите, используя Интернет?

a) До часа в день
b) До двух часов в день
c) До трех часов в день
d) Более трех часов в день
e) Не пользуюсь Интернетом. Переходите к вопросу № 19

13. Какие задачи Вы решаете при использовании Интернета? Выберите из списка.*

a) Использование электронной почты
b) Использование контента для работы/учебы
c) Использование контента в досуговых целях
d) Использование социальных сетей/мессенджеров
e) Другое_____

14. Является ли для Вас Интернет помехой при выполнении других задач, не связанных с Интернетом?

a) Да, полностью
b) Да, частично
c) Скорее да, чем нет
d) Скорее нет, чем да
e) Нет

15. Какое устройство Вы используете для выхода в сеть Интернет?*

a) Смартфон
b) Планшет
c) Компьютер/ноутбук

16. Каким образом Вы проверяете достоверность информации в сети Интернет?*

a) Пользуюсь проверенными источниками
b) Выясняю рейтинг сайта, на котором размещена информация
c) Выясняю информацию об авторе материала
d) Поиск других источников информации
e) Проверка фактического материала (наличие статистических данных, ссылок на авторитетные источники)
f) Использование специального ПО (**Trooclick и другие)**
g) Не проверяю достоверность информации
h) Другое_____

17. Какие образовательные интернет-порталы Вы используете?*

a) Edu.ru
b) Google Scholar
c) eLibrary
d) Cyberleninka
e) Другое_____
f) Не пользуюсь образовательными интернет-порталами

18. Какие информационные интернет-порталы Вы используете?*

a) Интернет-портал интеллектуальной молодежи (IPIM.ru)
b) Молодежный портал Xage.Ru
c) Молодежный научный портал «Ломоносов»
d) Российский Союз Молодежи
e) Другое_____
f) Не пользуюсь молодежными информационными интернет-порталами

19. Как Вы сами оцениваете уровень информационной безопасности?

a) Отлично. Переходите к Вопросу № 23
b) Хорошо
c) Удовлетворительно
d) Неудовлетворительно

20. Какие угрозы в сфере информационной безопасности, на Ваш взгляд, наиболее актуальны для молодежи?*

a) Нежелательное содержание
b) Азартные игры
c) Вредоносные и нежелательные программы
d) Мошенники, хакеры
e) Интернет-зависимость (виртуальное замещение реальности)
f) Сексуальные домогательства
g) Некорректность общения
h) Интернет-хулиганы
i) Затрудняюсь ответить

21. Почему, на Ваш взгляд, молодежь подвержена угрозам в сфере информационной безопасности?*

a) Не развита культура информационной безопасности
b) Нет критического мышления
c) Нет контроля со стороны родителей
d) Нет навыков противостояния мошенникам, хакерам
e) Нет самоконтроля и навыков планирования времени
f) Не подвержена информационной безопасности
g) Другое_____
h) Затрудняюсь ответить

22. Каким образом, на Ваш взгляд, необходимо повышать культуру информационной безопасности молодежи?*

a) Разработка нормативно-правового законодательства в сети Интернет
b) Мониторинг сети Интернет
c) Лицензирование информационной деятельности
d) Защита персональных данных
e) Самообразование по информационной безопасности
f) Проведение различных курсов по информационной безопасности
g) Другое_____

23. Укажите Ваш статус.

a) Обучающийся СОШ
b) Обучающийся СПО
c) Обучающийся ВУЗа
d) Другое_____

24. Укажите Ваш пол.

a) Мужской
b) Женский

25. Укажите количество полных лет (цифрами).

_____

26. Укажите Ваш район/город проживания.

a) Белгород
b) Белгородский район
c) Другое_____

Спасибо за участие!

Приложение 3

Визуализация результатов социологического опроса «Организация комплекса мероприятий по повышению уровня культуры информационной безопасности»

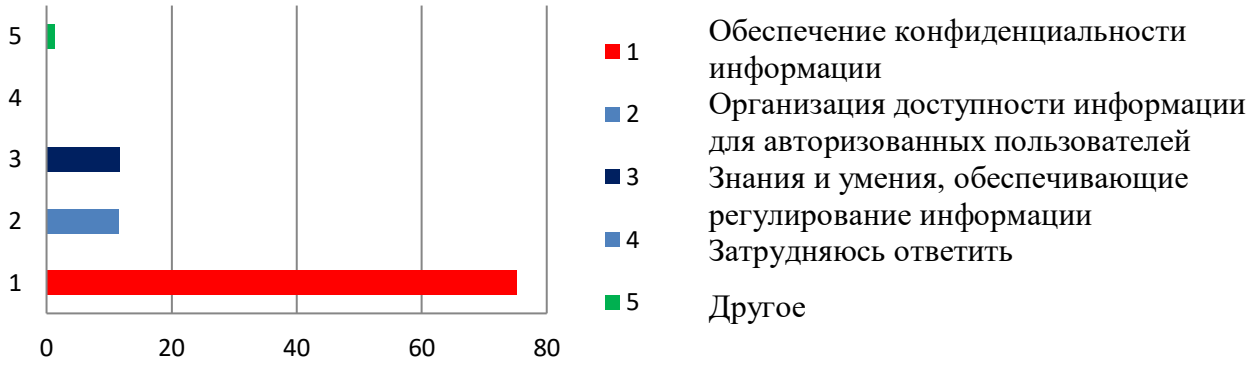

Диаграмма 1. Распределение ответов молодых людей на вопрос: «Что Вы понимаете под информационной безопасностью?»

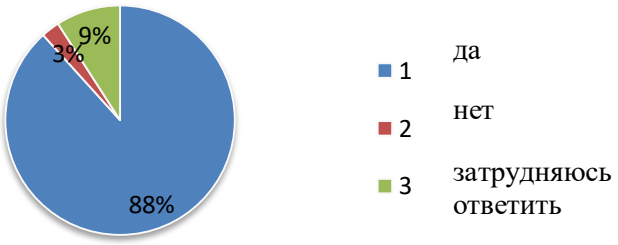

Диаграмма 2. Распределение ответов молодых людей на вопрос: «Необходимо ли правовое регулирование в сфере информационной безопасности?»

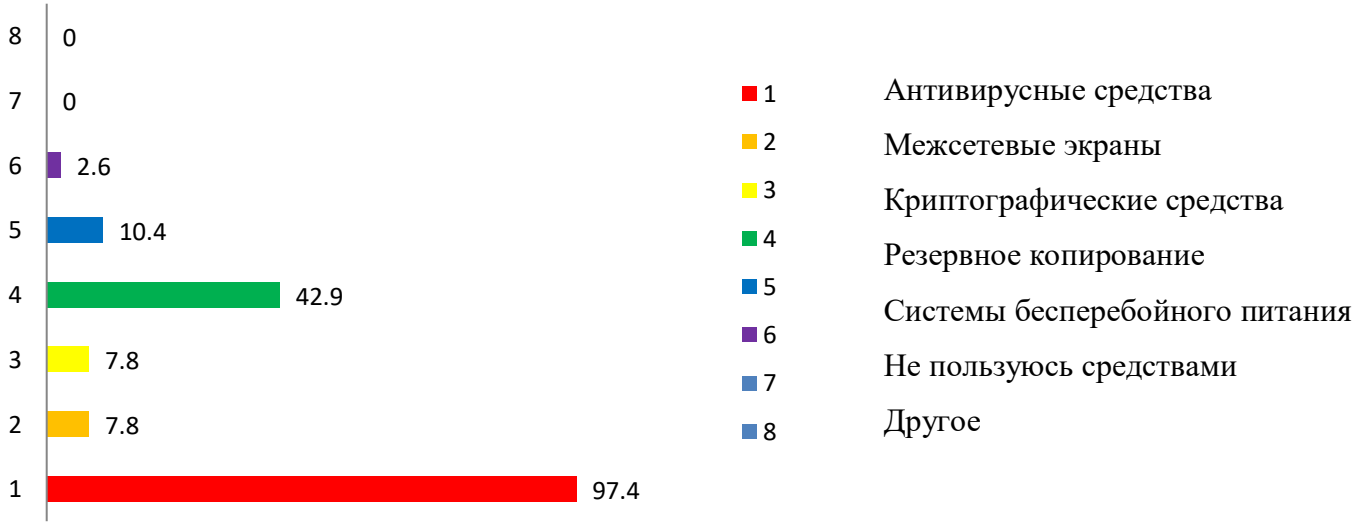

Диаграмма 3. Распределение ответов на вопрос: «Какие средства для организации информационной безопасности Вы используете?»

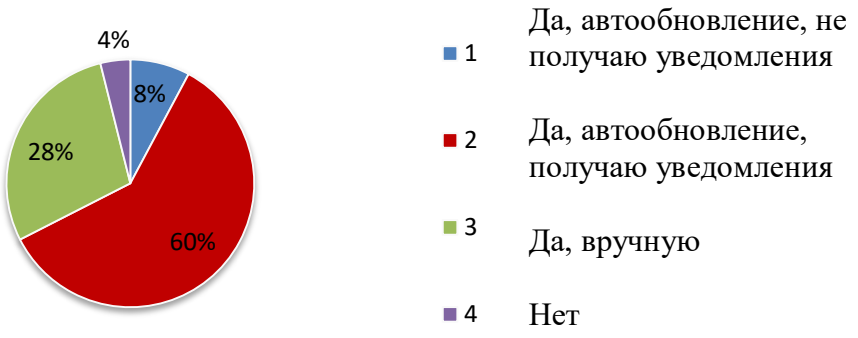

Диаграмма 4. Распределение ответов респондентов на вопрос: «Обновляете ли Вы программное обеспечение?»

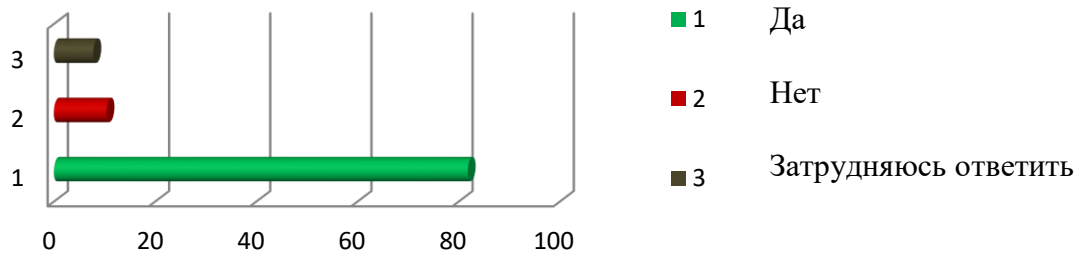

Диаграмма 5. Распределение ответов респондентов на вопрос: «Обновляете ли Вы программное обеспечение?»

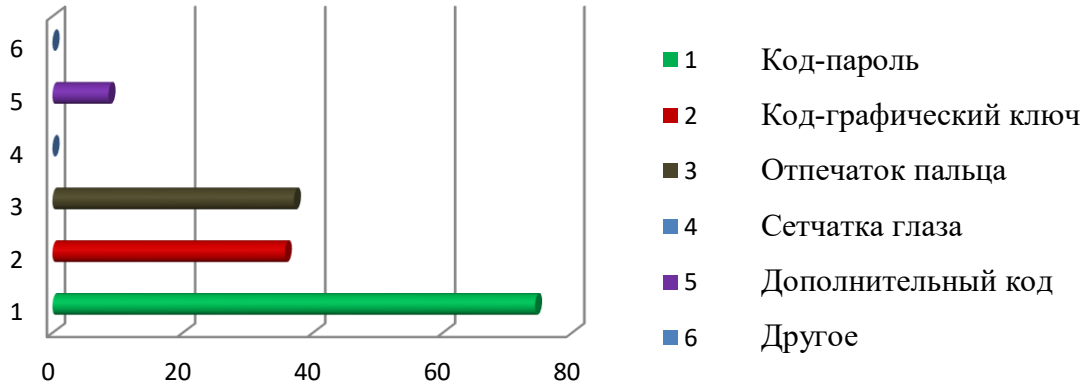

Диаграмма 6. Распределение ответов респондентов на вопрос: «Выберите из списка способы аутентификации, которыми Вы пользуетесь при использовании собственного устройства»

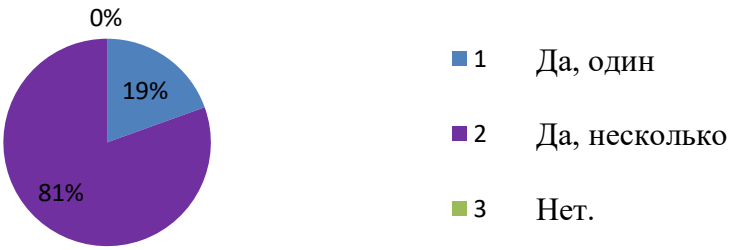

Диаграмма 7. Распределение ответов респондентов на вопрос: «Имеете ли Вы аккаунт/ы в социальных сетях (мессенджерах)?»

Диаграмма 8. Распределение ответов респондентов на вопрос: «Как часто Вы пользуетесь социальными сетями (мессенджерами)?»

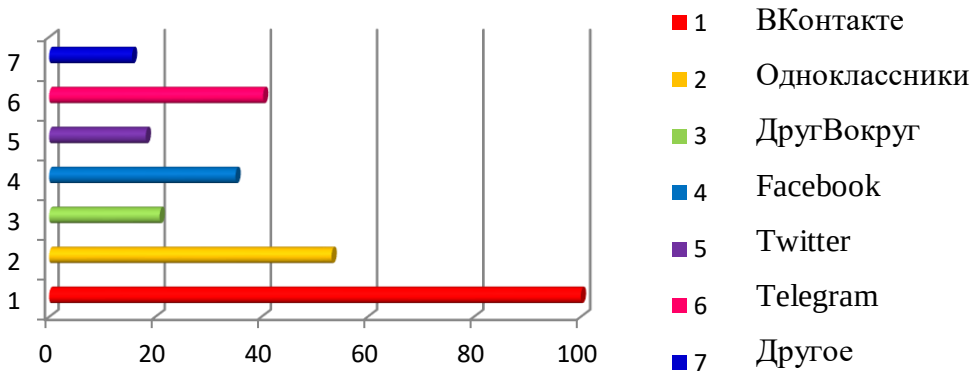

Диаграмма 9. Распределение ответов респондентов на вопрос: «Выберите название той социальной сети (мессенджера), где у Вас есть аккаунт/ы»

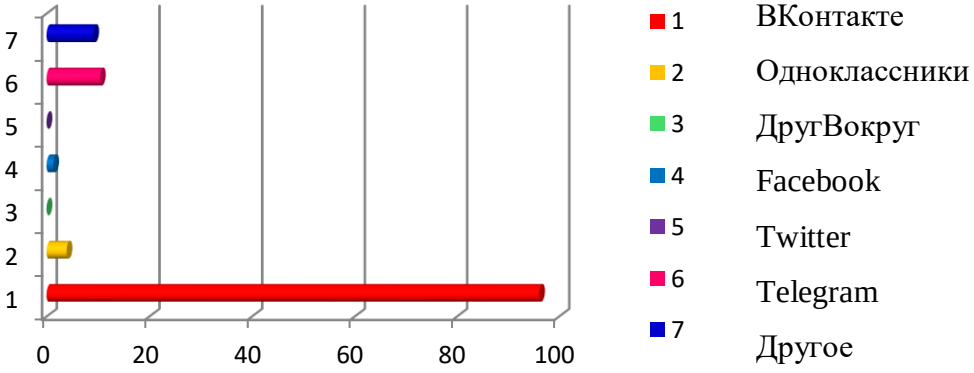

Диаграмма 10. Распределение ответов респондентов на вопрос: «Какую социальную сеть (мессенджер) Вы используете чаще всего?»

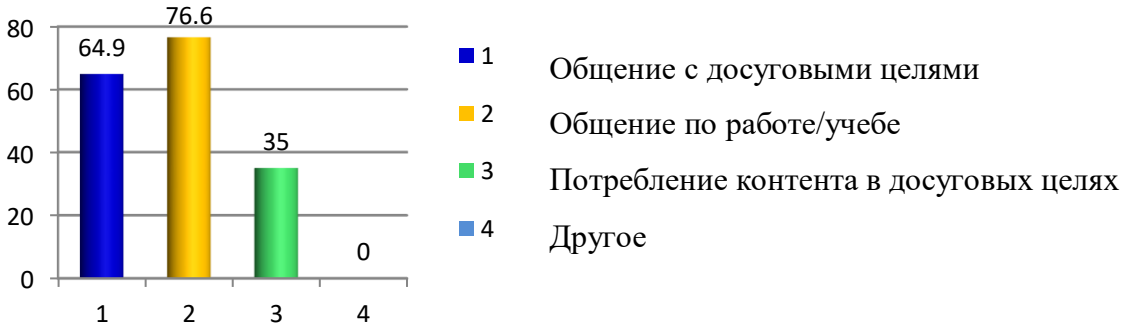

Диаграмма 11. Распределение ответов респондентов на вопрос: «С какой целью Вы используете социальную сеть (мессенджер)?»

Диаграмма 12. Распределение ответов респондентов на вопрос: «Сколько времени в день Вы проводите, используя Интернет?»

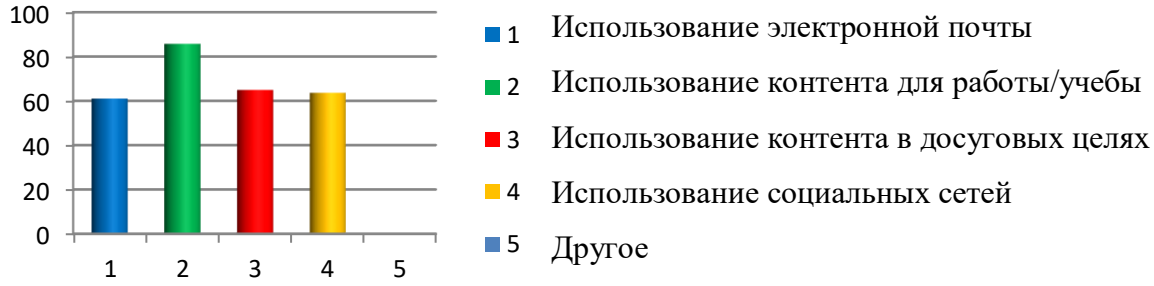

Диаграмма 13. Распределение ответов респондентов на вопрос: «Какие задачи Вы решаете при использовании Интернета?»

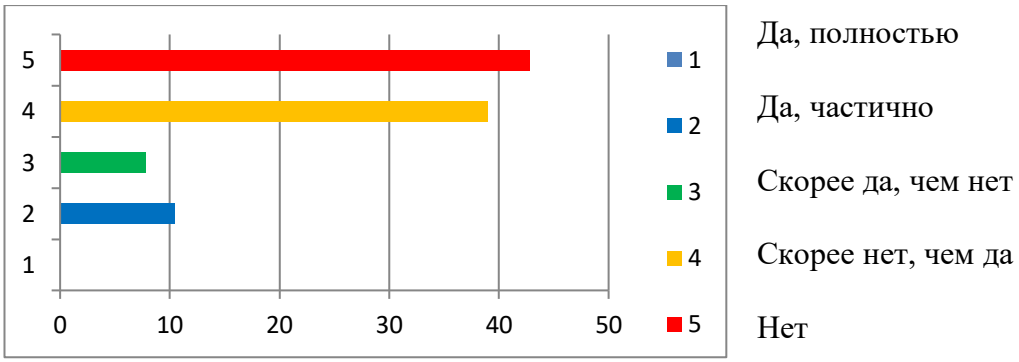

Диаграмма 14. Распределение ответов респондентов на вопрос: «Является ли для Вас Интернет помехой при выполнении других задач, не связанных с Интернетом?»

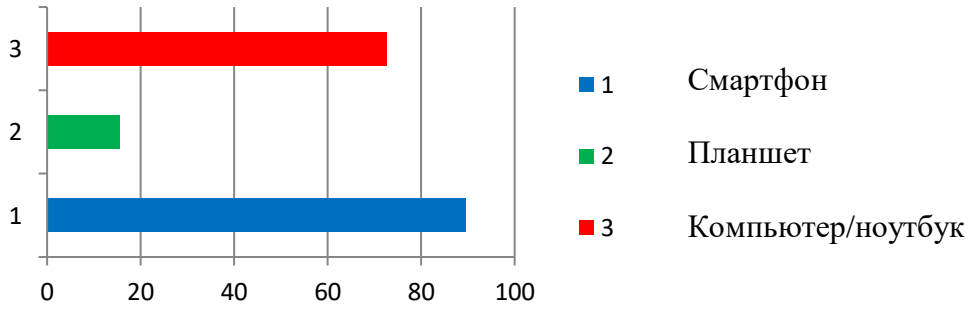

Диаграмма 15. Распределение ответов респондентов на вопрос: «Какое устройство Вы используете для выхода в сеть Интернет?»

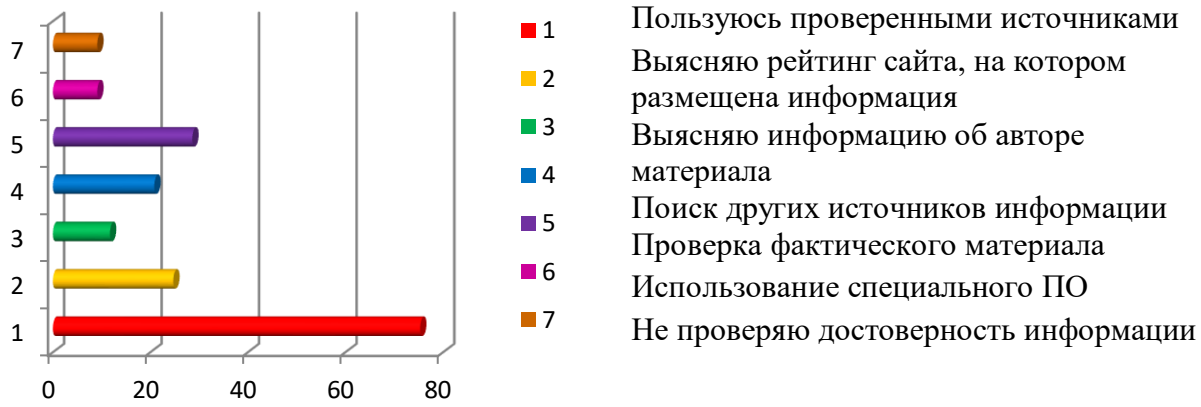

Диаграмма 16. Распределение ответов респондентов на вопрос: «Каким образом Вы проверяете достоверность информации в сети Интернет?»

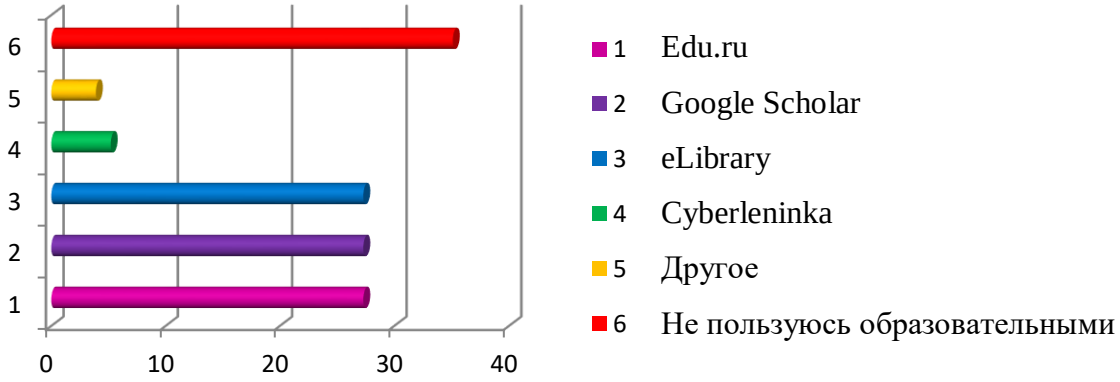

Диаграмма 17. Распределение ответов респондентов на вопрос: «Какие образовательные интернет-порталы Вы используете?»

Диаграмма 18. Распределение ответов респондентов на вопрос: «Какие информационные интернет-порталы Вы используете?»

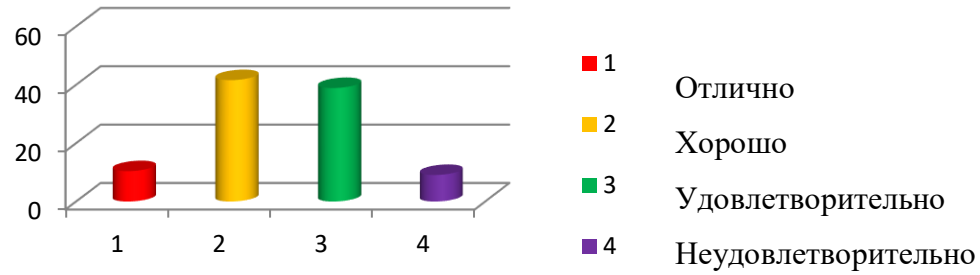

Диаграмма 19. Распределение ответов респондентов на вопрос: «Как Вы сами оцениваете уровень информационной безопасности?»

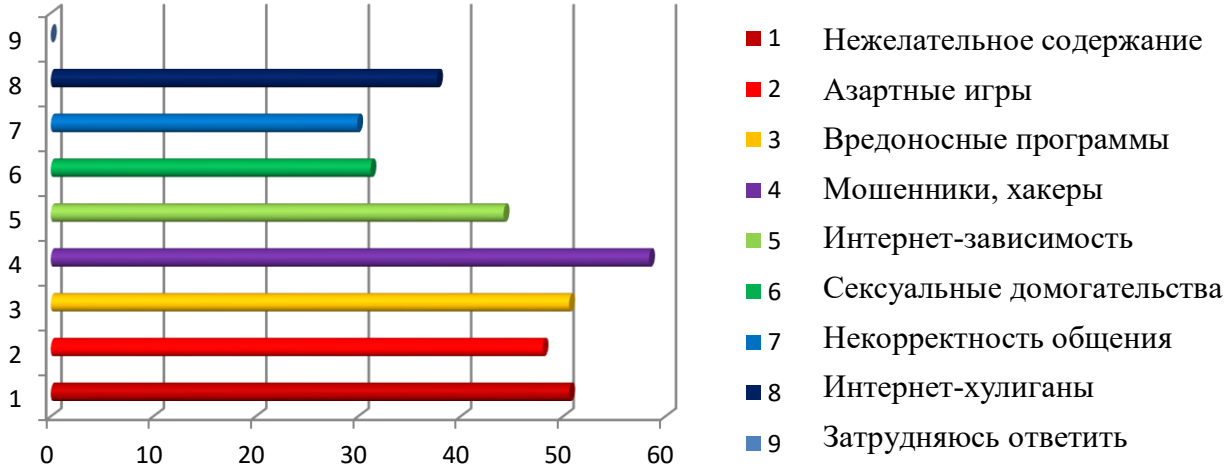

Диаграмма 20. Распределение ответов респондентов на вопрос: «Какие угрозы в сфере информационной безопасности, на Ваш взгляд, наиболее актуальны для молодежи?»

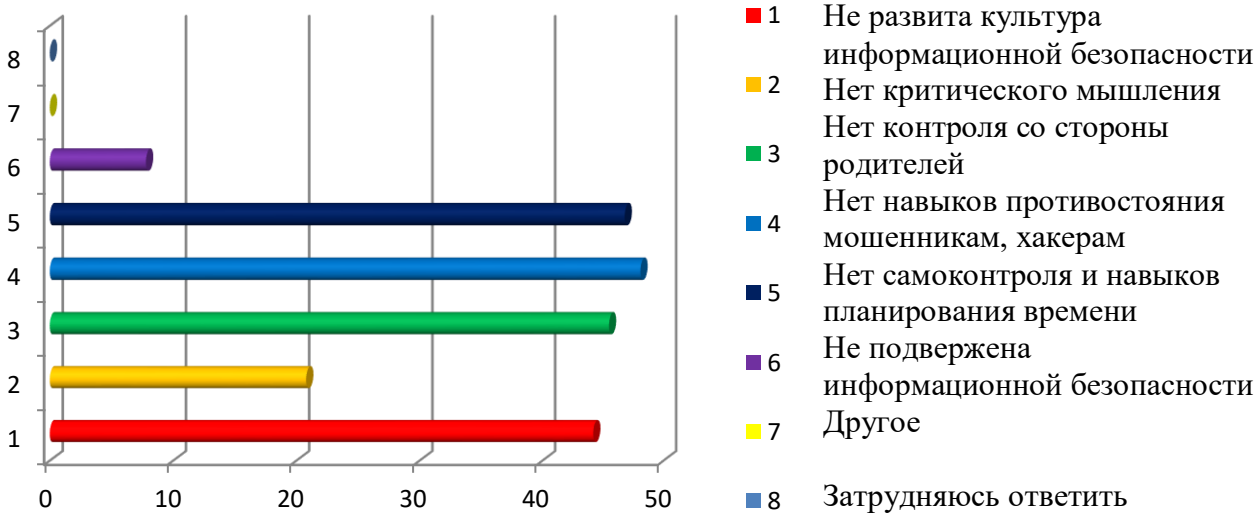

Диаграмма 21. Распределение ответов респондентов на вопрос: «Почему, на Ваш взгляд, молодежь подвержена угрозам в сфере информационной безопасности?»

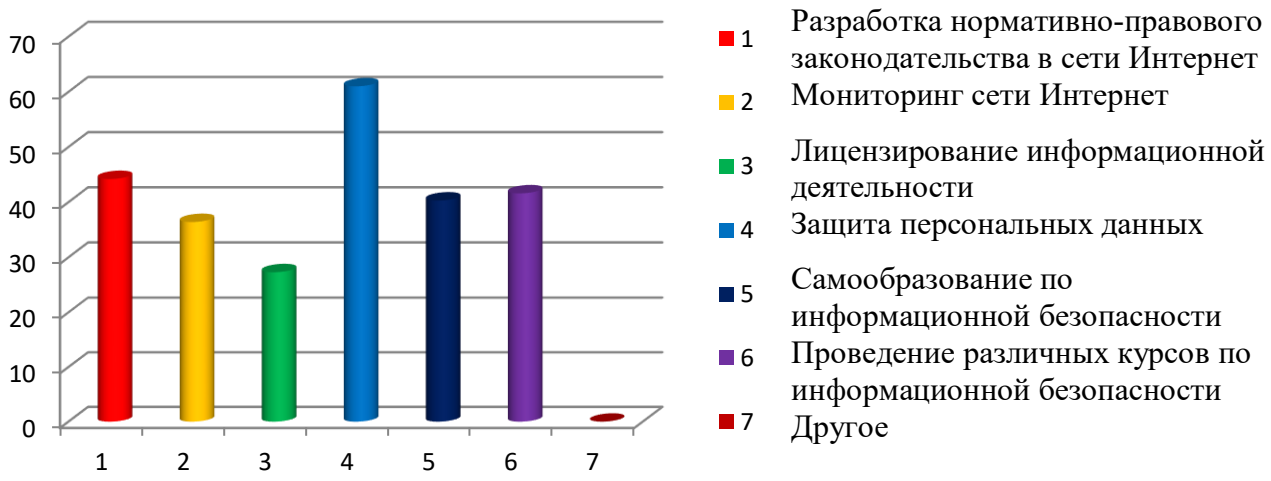

Диаграмма 22. Распределение ответов респондентов на вопрос: «Каким образом, на Ваш взгляд, необходимо повышать культуру информационной безопасности молодежи?»

Приложение 4. Апробация результатов исследования

СибАК
sibac.info

СЕРТИФИКАТ
участника

XXXIX международная студенческая
научно-практическая конференция

«Научное сообщество студентов XXI столетия»

МЕЖДИСЦИПЛИНАРНЫЕ ИССЛЕДОВАНИЯ

Почапский Александр Михайлович

Научная работа:
«РОССИЙСКИЙ И ЗАРУБЕЖНЫЙ ОПЫТ ФОРМИРОВАНИЯ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МОЛОДЕЖИ»

Научный руководитель:
Говоруха Наталья Сергеевна

Председатель оргкомитета
канд. мед. наук, д-р психол. наук,
профессор, академик
Международной академии наук
педагогического образования

Ассоциация научных сотрудников «Сибирская академическая книга» ИНН 5404255395

Н.В. Дмитриева

Новосибирск
2018 год

СибАК
sibac.info

СЕРТИФИКАТ
участника

XLIII международная студенческая
научно-практическая конференция

«Научное сообщество студентов XXI столетия»

МЕЖДИСЦИПЛИНАРНЫЕ ИССЛЕДОВАНИЯ

Почапский Александр Михайлович

Научная работа:
«РЕЗУЛЬТАТЫ СОЦИОЛОГИЧЕСКОГО ИССЛЕДОВАНИЯ «ОПРЕДЕЛЕНИЕ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МОЛОДЕЖИ»»

Научный руководитель:
Говоруха Наталья Сергеевна

Председатель оргкомитета
канд. мед. наук, д-р психол. наук,
профессор, академик
Международной академии наук
педагогического образования Н.В. Дмитриева

Новосибирск
2018 год