МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА АВТОМОБИЛЬНОГО ТРАНСПОРТА, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ТЕХНИЧЕСКИМ ДИСЦИПЛИНАМ

Формирование основ кибербезопасности у студентов профессиональной образовательной организации при преподавании общеобразовательной дисциплины

Выпускная квалификационная работа по направлению
44.04.04 Профессиональное обучение (по отраслям)
Направленность программы магистратуры
«Управление информационной безопасностью в профессиональном образовании»
Форма обучения заочная

Проверка на объем заимствований:
70,4 % авторского текста

Работа рекомендована к защите
«27» 01 2025 г.
Зав. кафедрой АТИТ и МОТД
_____ Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Люст Татьяна Николаевна

Научный руководитель:
к.п.н., доцент
Диденко Галина Александровна

Челябинск
2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Вопросы обеспечения информационной и кибербезопасности являются одной из ключевых проблем в современной России.

Современный человек живет в эпоху, когда доступ к Интернету стал неотъемлемой частью повседневной жизни. Благодаря проводным и беспроводным технологиям, таким как Wi-Fi и мобильные сети, мы можем использовать различные устройства — компьютеры, планшеты и смартфоны — для связи с миром. Это изобретение кардинально изменило наше восприятие информации.

Изобретение Интернета дало нам много возможностей, например, таких как, быстрый и неограниченный доступ к информации, обучение без отрыва от профессиональной деятельности, дистанционное повышение квалификации, получение дополнительного образования; новые возможности для работы, общения и досуга, получение образования людьми с ограниченными возможностями и особенностями здоровья и т.д.

В то же время вместе со значительным ростом возможностей проникновение ИКТ во все сферы жизни вызывает возникновение ряда новых и развитие некоторых существующих угроз личности, обществу и государству, таких как, например, подделка компьютерной информации; компьютерное мошенничество и саботаж; несанкционированный доступ к информации; повреждение данных или программ; нарушение авторских прав. Атаки в киберпространстве, разные способы вмешательства в работу компьютерных систем и сетей, включая их намеренное повреждение или разрушение, представляют собой одну из самых серьезных угроз в информационной индустрии. Кибератака может варьироваться в разных масштабах: от загрузки компьютерных вирусов до взлома транснациональных корпораций с целью кражи финансовой или конфиденциальной информации у клиентов.

Согласно ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Терминология, концептуальные положения и модели (Издание с Поправкой). Часть 1-1, атака – это «посягательство на систему, которое является следствием продуманного планирования, т.е. умышленного действия, представляющее собой продуманную попытку (особенно в плане метода или стратегии) обойти сервисы безопасности и нарушить политику безопасности системы» [19]. Атаки могут приводить к кражам личной информации человека и организаций, кражам финансовой информации и интеллектуальной собственности, потерям данных, веб-трафика и даже бизнеса в результате действия этих атак.

Актуальность написания выбранной темы обусловлена внедрением информационных технологий во все сферы жизнедеятельности человека и непрерывным ростом числа инцидентов в сфере информационной безопасности – от утечек информации до кибератак и кибертерроризма.

Авторы Доктрины информационной безопасности РФ приводят статистику, что «в настоящее время население России составляет 146,4 млн. человек, из которых 30,2 млн. человек – несовершеннолетние (20,6 процента населения), из них 27 млн. человек являются активными пользователями информационно-телекоммуникационной сети «Интернет». Указанная аудитория является крайне уязвимой с точки зрения информационной безопасности. В связи с высокой степенью анонимности интернет-пространства и возможностью выстраивания общения с использованием псевдонимов и нескольких профилей риск проявления асоциальных форм поведения в цифровой среде увеличивается» [7].

В Доктрине информационной безопасности Российской Федерации указывается, что обеспечение информационной безопасности (ИБ) РФ играет ключевую роль в обеспечении национальной безопасности РФ.

При этом одним из приоритетных направлений государственной политики в области обеспечения информационной безопасности РФ

является совершенствование подготовки кадров, развитие образования в области информационной безопасности. Особую роль в решении этих задач играют учебные заведения.

Образовательные организации, осознающие важность этой проблемы, могут внести значительный вклад в развитие культуры кибербезопасности среди обучающейся молодежи, что, в свою очередь, повысит общую безопасность в обществе.

Все это свидетельствует о том, что тема нашего исследования является актуальной: «Формирование основ кибербезопасности у студентов профессиональной образовательной организации при преподавании общеобразовательной дисциплины».

Цель исследования состоит в выявлении, теоретическом обосновании и экспериментальной проверке комплекса мероприятий формирования основ кибербезопасности обучающихся профессиональной образовательной организации (ПОО).

Объект исследования: процесс профессиональной подготовки обучающихся колледжа.

Предмет исследования: процесс формирования кибербезопасности у обучающихся ПОО в ходе профессиональной подготовки при преподавании общеобразовательной учебной дисциплины Информатика.

Гипотеза исследования: формирование основ кибербезопасности у студентов профессиональной образовательной организации будет более эффективным, если выявить и реализовать комплекс мероприятий по основам кибербезопасности.

В соответствии с объектом, предметом и целью исследования были поставлены следующие задачи:

1. Изучить современное состояние проблемы кибербезопасности.
2. Определить содержание основных понятий исследуемой проблемы.

3. Изучить состояние информационной среды ГБПОУ «Южно-Уральский государственный технический колледж».

4. Разработать и экспериментально проверить комплекс мероприятий по формированию основ кибербезопасности обучающихся профессиональной образовательной организации на примере ГБПОУ «Южно-Уральский государственный технический колледж».

Методологическая база педагогического исследования основана на ряде ключевых идей и положений, взятых из различных подходов и теорий. Рассмотрим каждую из них подробнее:

1) Системный подход (Аверьянов А.Н., Уварина Н.В. и др.). Системный подход рассматривает педагогический процесс как сложную систему, состоящую из множества взаимосвязанных элементов. Этот подход помогает увидеть общую картину и понять, как изменения в одной части системы влияют на всю систему в целом.

2) Деятельностный подход (Асмолов А.Г., Щедровицкий Г.П. и др.). Деятельностный подход фокусируется на активности и взаимодействии субъектов образовательного процесса. Он утверждает, что обучение происходит через активную деятельность, и акцентирует внимание на развитии у обучающихся компетенций самостоятельного мышления и действия.

3) Теория педагогического эксперимента (Бухарова Г.Д., Подласый И.П., Яковлева Н.О., и др.) Педагогический эксперимент позволяет проверить гипотезы и оценить эффективность новых педагогических методов и технологий. Он важен для научного обоснования и внедрения инноваций в образовательный процесс.

4) Интерактивные образовательные технологии (Голованова И.И., Рафикова Р.С. и др.). Интерактивные образовательные технологии предполагают активное вовлечение обучающихся в процесс обучения через использование современных технических средств и методов. Они

способствуют развитию критического мышления, коммуникативных навыков и творческой активности.

5) Цифровизация образования (Блинов В.И., Роберт И.В. и др.) Цифровизация образования связана с внедрением цифровых технологий в образовательный процесс. Она охватывает использование электронных учебников, онлайн-курсов, платформ для дистанционного обучения и других цифровых инструментов, которые повышают доступность и качество образования.

Методологическая база педагогического исследования, основанная на перечисленных выше подходах и теориях, позволяет комплексно подходить к изучению и совершенствованию образовательного процесса. Такой многоаспектный взгляд помогает учитывать разнообразные факторы, влияющие на обучение, и разрабатывать эффективные стратегии для достижения лучших результатов.

Методологической основой исследования кибербезопасности являются фундаментальные работы в области ИБ:

1) Доктрина информационной безопасности Российской Федерации.
2) Концепция информационной безопасности детей в РФ.
3) Проект Концепция стратегии кибербезопасности РФ.
4) Стратегия развития информационного общества в РФ.

Новизна работы состоит в формировании информационной безопасности обучающихся профессиональной образовательной организации и подготовке выпускников колледжа к дальнейшей безопасной профессиональной и личной информационной деятельности в информационном обществе.

Теоретическая значимость исследования определяется расширением научных знаний в области методов обеспечения информационной безопасности и формирования основ кибербезопасности у студентов профессиональных образовательных организаций при изучении общеобразовательной дисциплины.

Практическая значимость состоит в разработанном комплексе мероприятий для обучающихся ГБПОУ «ЮУрГТК», которая может быть использована в практике для формирования основ информационной и кибербезопасности студентов данной профессиональной образовательной организацией.

Методы исследования:

1) Теоретические (понятийно-терминологический и сравнительно-сопоставительный анализ научно-педагогической и методической литературы по вопросам кибербезопасности, анализ законодательства в сфере информационной безопасности).

2) Эмпирические (педагогический эксперимент, наблюдение, анкетирование).

3) Методы обработки и интерпретации результатов.

База исследования: Государственное бюджетное профессиональное образовательное учреждение «Южно-Уральский государственный технический колледж» (ГБПОУ «ЮУрГТК»).

Основные этапы исследования.

Исследование проводилось в три этапа в период с 2023 по 2024 гг. На первом этапе формулировались тема исследования и план диссертации, осуществлялась формулировка гипотезы, постановка цели и задач. На этом этапе проводилось изучение научно-педагогической и технической литературы, отбор источников информации, анализ современного состояния кибербезопасности и изучение методики формирования кибербезопасности у обучающихся ПОО, публикация научных статей по теме исследования.

На втором этапе проводилась экспериментальная работа, анализ исследования, обработка данных, разработка рекомендаций по формированию основ кибербезопасности у студентов колледжа при изучении общеобразовательной учебной дисциплины Информатика, а

также текстовое оформление материалов исследования, формулировка выводов.

На третьем этапе анализировались и обобщались полученные результаты экспериментальной работы, осуществлялось текстовое оформление материалов исследования, формулировались выводы.

Основные положения и результаты работы были представлены на Областной научно-практической конференции «Актуальные проблемы профессионального образования», организованной областным методическим объединением преподавателей УГС «Архитектура», УГС «Техника и технологии строительства» Челябинской области в виде публикации статей: в 2024 году «Формирование информационной безопасности обучающихся профессиональной образовательной организации»; в 2023 году статья «Развитие конкретных психологических профессионально важных качеств как фактор развития профессионализма». По теме работы опубликованы две печатные работы.

Личное участие соискателя состоит в анализе системы информационной среды при формировании основ кибербезопасности у обучающихся ПОО, а также разработке комплекса практических мероприятий по формированию основ кибербезопасности у студентов ГБПОУ «ЮУрГТК» при аудиторной и внеаудиторной работе при преподавании общеобразовательной учебной дисциплины «Информатика». Результаты работы внедрены в практику деятельности ГБПОУ «Южно-Уральский государственный технический колледж».

Структура выпускной квалификационной работы. Выпускная квалификационная работа состоит из введения, двух глав, заключения, списка использованных источников, приложений. Основная часть работы изложена на 91 странице машинописного текста, в число которых входит 17 рисунков и 8 таблиц. Список использованных источников содержит 61 наименование, приложения занимают 37 страниц.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ФОРМИРОВАНИЯ ОСНОВ КИБЕРБЕЗОПАСНОСТИ

1.1 Современное состояние проблемы кибербезопасности

Информатизация экономической и социально-политической деятельности Российской Федерации и, как следствие, стремительное развитие информационно-телекоммуникационных систем и технологий сопровождается повышенным вниманием к информации и информационным ресурсам, как со стороны иностранных государств, так и со стороны преступных элементов и граждан, не имеющих доступа к ней. Поэтому, одной из первоочередных задач, стоящих перед правовым государством, является обеспечение информационной безопасности личности, общества и государства.

Информационные ресурсы нации формируют и составляют информационный потенциал общества, который становится таким же важным экономическим и социальным фактором развития, как энергетический, промышленный, образовательный и оборонный потенциал.

Информационный потенциал общества включает сеть научно-исследовательских, учебных, административных, коммерческих и других организационных и социальных институтов, деятельность которых содействует эффективному использованию информационных ресурсов и индустриально-технологический комплекс средств информатизации и компьютеризации. Также для подготовки для этих целей необходимо достаточное количество специалистов соответствующего профиля. В связи с этим особую актуальность приобретает проблема повышения информационной культуры общества, то есть степени его подготовки к эффективному использованию информационных ресурсов и продуцированию новых знаний.

Кандидат экономических наук, доцент кафедры «Предпринимательство и маркетинг» ФГБОУ ВПО «Госуниверситет – УНПК» Артемов А.В., автор курса лекций по информационной безопасности, считает, что в современном мире информация играет ключевую роль не только в экономике, но и в политике, социальной сфере и даже военном деле. Государства активно используют информационные ресурсы для достижения своих целей, будь то укрепление экономики, повышение уровня жизни граждан или обеспечение обороноспособности. Информация становится стратегическим активом, который необходимо защищать от несанкционированного доступа, утечек и кибератак. В условиях глобализации и развития цифровых технологий угрозы информационной безопасности становятся всё более разнообразными и сложными. Поэтому государство должно уделять особое внимание защите информационных систем, данных и сетей, чтобы предотвратить возможные негативные последствия для общества и экономики. Защита информации действительно превратилась в одну из важнейших государственных задач, поскольку она напрямую связана с обеспечением суверенитета страны, её стабильности и процветания [20].

В Российской Федерации фундаментом правового регулирования отношений в Интернете является Конституция РФ, закрепившая такие положения, как право каждого гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ст.29). А статья 71 гласит, что «в ведении Российской Федерации находятся …. обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных» [1].

Таким образом, государство берет на себя ответственность за информационную безопасность всех граждан страны. В Российской Федерации активно предпринимаются шаги по усилению информационной безопасности. Важнейшими из них стали следующие меры:

1) Принятие федеральных законов, например, таких как:

– Федеральный закон «О безопасности». Этот закон устанавливает правовые основы обеспечения безопасности государства, общества и личности. Он определяет полномочия органов власти в вопросах обеспечения безопасности, а также принципы и механизмы ее реализации [11],

– Федеральный закон «О государственной тайне». Закон регулирует порядок отнесения сведений к государственной тайне, их засекречивания, рассекречивания и защиты. Он также устанавливает ответственность за разглашение государственной тайны [2].

2) Формирование нормативно-правовой базы. Начата разработка и реализация нормативных актов, направленных на укрепление информационной безопасности. Это включает в себя регламентацию деятельности в информационной сфере, разработку стандартов и требований к защите информации.

3) Механизмы реализации. Ведутся работы по созданию эффективных механизмов реализации принятых законов. Это включает в себя разработку методических рекомендаций, инструкций и руководств для государственных органов и организаций, а также контроль за соблюдением установленных норм.

4) Подготовка законодательных проектов. Завершены работы над проектами законодательных актов, регулирующих деятельность в информационной сфере. Эти проекты направлены на усиление контроля и защиты информации, предотвращение киберпреступлений и обеспечение безопасности в Интернете.

Все эти меры направлены на повышение уровня информационной безопасности в стране, защиту национальных интересов и обеспечение стабильности в условиях возрастающего числа киберугроз.

Согласно Федеральному закону «О безопасности», «государственная политика в области обеспечения безопасности является частью внутренней

и внешней политики Российской Федерации и представляет собой совокупность скоординированных и объединенных единым замыслом политических, организационных, социально-экономических, военных, правовых, информационных, специальных и иных мер. Основные направления государственной политики в области обеспечения безопасности определяет Президент Российской Федерации» [11].

Создание Государственной системы защиты информации (ГСЗИ) в Российской Федерации стало ключевым элементом в укреплении информационной безопасности на государственном уровне. Эта система направлена на противодействие иностранным техническим разведкам и предотвращение утечки информации по техническим каналам связи. Основные аспекты этой системы включают:

1) Защита от иностранных технических разведок. ГСЗИ включает комплекс мер, направленных на предотвращение несанкционированного доступа к информации со стороны иностранных государств. Это достигается путем использования специальных технических средств, шифрования данных, а также постоянного мониторинга и анализа активности в информационных системах.

2) Предотвращение утечки информации по техническим каналам связи. Важной частью ГСЗИ являются механизмы защиты каналов передачи данных, включая телефонную связь, интернет и другие виды коммуникаций. Эти меры включают использование защищенных линий связи, шифрование трафика и контроль доступа к сетевым ресурсам.

Кроме того, важную роль играют системы лицензирования деятельности организаций в области защиты информации и сертификации средств защиты информации. Они обеспечивают:

1) Лицензирование деятельности. Организации, занимающиеся защитой информации, обязаны получать лицензии на свою деятельность. Это гарантирует, что компании соответствуют установленным стандартам

и обладают необходимыми компетенциями для выполнения работ в данной области.

2) Сертификация средств защиты информации. Средства защиты информации проходят обязательную сертификацию, которая подтверждает их соответствие требованиям безопасности. Это позволяет гарантировать надежность используемых технологий и снижает вероятность утечек или взломов.

Совместно эти меры способствуют созданию надежной и эффективной системы защиты информации, обеспечивая безопасное функционирование органов государственной власти, государственных и общественных организаций, а также предприятий [33].

Анализ состояния информационной безопасности в Российской Федерации выявил значительные пробелы и недостатки, несмотря на усилия по её совершенствованию. Уровень информационной безопасности пока не соответствует жизненно важным потребностям личности, общества и государства по нескольким причинам:

1) Недостаточная осведомленность пользователей. Несмотря на проводимые тренинги и образовательные программы, многие граждане и сотрудники организаций всё ещё недостаточно осведомлены о базовых принципах информационной безопасности. Это приводит к тому, что люди становятся жертвами фишинговых атак, используют слабые пароли и пренебрегают другими важными правилами защиты информации.

2) Ограниченная техническая оснащенность. Не все государственные учреждения и предприятия имеют доступ к современным средствам защиты информации. Некоторые продолжают использовать устаревшие технологии, которые не способны эффективно противостоять современным киберугрозам.

3) Высокая сложность и изменчивость угроз. Киберпространство постоянно эволюционирует, и новые угрозы появляются каждый день. Традиционные подходы к обеспечению безопасности уже не всегда

эффективны против сложных и адаптивных атак, проводимых профессиональными хакерскими группами.

4) Отсутствие комплексного подхода. Информационная безопасность требует комплексного подхода, включающего технические, организационные и правовые меры. В некоторых случаях этот подход не реализуется должным образом, что приводит к уязвимости отдельных звеньев системы защиты.

5) Недостаточно развитое законодательство. Законодательная база в области информационной безопасности нуждается в дальнейшем развитии и адаптации к новым вызовам. Существуют пробелы в регулировании, которые затрудняют эффективное управление рисками и реагирование на инциденты.

6) Нехватка квалифицированных кадров. Недостаточное количество специалистов в области информационной безопасности создает дефицит профессиональных ресурсов, необходимых для разработки и внедрения эффективных мер защиты.

7) Глобальная взаимосвязанность. Россия интегрирована в мировую экономику и информационное пространство, что делает её уязвимой для глобальных киберугроз. Международное сотрудничество в области информационной безопасности необходимо для эффективного противостояния транснациональным угрозам.

Таким образом, хотя проделана значительная работа по совершенствованию информационной безопасности, остаётся много нерешённых проблем, требующих дальнейшего внимания и усилий. Для повышения уровня информационной безопасности необходимы дополнительные инвестиции, развитие кадрового потенциала и совершенствование правовой базы.

Сегодняшние условия социально-экономического и политического развития общества и государства вызывают обострение противоречий между потребностями общества в расширении свободного обмена

информацией и необходимостью сохранения определенных ограничений на ее распространение со стороны государства. Отсутствие действенных механизмов регулирования информационных отношений в обществе и государстве приводит к негативным последствиям.

Отставание отечественных информационных технологий вынуждает идти по пути закупок незащищенной импортной техники, в результате чего повышается вероятность несанкционированного доступа к банкам и базам данных, а также возрастает зависимость Российской Федерации от иностранных производителей информационных технологий и телекоммуникационной и компьютерной техники.

Положение дел с обеспечением информационной безопасности в Российской Федерации таково, что не позволяет ей на равноправной основе включиться в мировую информационную систему и требует решения следующих ключевых проблем:

1) Формирования нормативно-правовой базы обеспечения информационной безопасности, регламента информационного обмена для органов государственной власти и государственного управления, предприятий и организаций, нормативного закрепления ответственности должностных лиц и граждан за соблюдение требований информационной безопасности.

2) Комплексного исследования деятельности личного состава информационных систем, в том числе методов повышения мотивации, морально-психологической устойчивости и социальной защищенности сотрудников, работающих с конфиденциальной информацией.

3) Разработки механизмов реализации прав физических и юридических лиц на информацию.

4) Разработки аппаратных и программных средств, обеспечивающих комплексное решение задач защиты информации.

5) Формирования системы информационной безопасности, являющейся составной частью общей системы национальной безопасности страны.

Решение вышеперечисленных ключевых проблем информационной безопасности должно осуществляться на основе соответствующей государственной политики. Основополагающим документом, определяющим стратегию обеспечения информационной безопасности на национальном уровне, является Доктрина информационной безопасности Российской Федерации, в которой подчеркивается важность обеспечения независимого присутствия России в мировом информационном пространстве и противодействия дезинформации [7].

Система информационной безопасности России продолжает активно развиваться, но этому препятствует ряд факторов:

1. Проблема технологической независимости. Для ее решения необходимо развивать отечественное аппаратное и программное обеспечение, готовить высококвалифицированных специалистов в области информационной безопасности и создавать собственные каналы связи. Важнейшую роль играют четкая нормативно-правовая база, регулирующая вопросы управления рисками в киберпространстве и эффективное взаимодействие между ведомствами разной подчиненности. Серьезной проблемой остается зависимость от зарубежного оборудования и технологий, что делает российскую систему кибербезопасности уязвимой.

2. Несовершенство защиты персональных данных. Одной из основных проблем является недостаточная осведомленность организаций о требованиях законодательства и ответственности за его нарушение. Многие компании либо недооценивают риски, связанные с утечками данных, либо считают затраты на защиту информации чрезмерно высокими. Кроме того, существуют сложности технического характера. Не все организации имеют достаточные ресурсы для внедрения современных средств защиты информации, таких как шифрование данных, системы

мониторинга и предотвращения вторжений. Также могут возникать трудности при интеграции новых технологий в уже существующие ИТ-инфраструктуры. Ещё одной проблемой является человеческий фактор. Даже при наличии технических мер защиты сотрудники могут случайно или намеренно нарушать правила обработки персональных данных, что также может привести к утечкам.

3. Несовершенство защиты информации в образовании и социальной сфере. Обеспечение кибербезопасности в образовании и социальной сфере является важной задачей, решение которой осложняется некоторыми причинами. Помимо трудностей в регулировании деятельности международных социальных сетей и распространения нежелательного контента, существуют и другие проблемы: нехватка квалифицированных кадров в сфере кибербезопасности; недостаточное финансирование мероприятий по обеспечению кибербезопасности в образовательных учреждениях; низкий уровень киберграмотности населения, особенно среди подрастающего поколения.

Опасность: Подрастающее поколение является одной из наиболее уязвимых категорий в киберпространстве. Они могут стать жертвами мошенничества, кибербуллинга, вербовки в экстремистские организации и других киберугроз. Низкий уровень кибербезопасности в образовательных организациях делает их привлекательной целью для киберпреступников, которые могут похитить персональные данные всех участников образовательного процесса, нарушить работу образовательного процесса.

Согласно ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения», «персональные данные - это любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения,

адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация» [18].

4. Вызовы информационной безопасности в международном контексте. Действительно, события последних лет привели к усилению кибертерроризма и использованию информационных технологий для дестабилизации политической обстановки в разных странах мира. Рост напряженности между странами в киберпространстве, включая гонку кибервооружений; отсутствие единых международных норм и правил в сфере кибербезопасности; проблема атрибуции кибератак, то есть установления их заказчика и источника [51].

Проблемы информационной и кибербезопасности становятся все более актуальными и требуют комплексного подхода к решению. Важно развивать сотрудничество между государством, обществом и бизнесом для создания безопасной и устойчивой информационной среды.

Несмотря на активные усилия России по укреплению информационной безопасности, статистика показывает, что ситуация с киберугрозами остается напряженной. Данные по кибератакам в 2022 году свидетельствуют о том, что их количество растет, меняется их характер; атаки носят целенаправленный характер и основными мишенями для киберпреступников являются государственные органы, промышленные и оборонные предприятия.

По заявлению начальника Бюро специальных технических мероприятий МВД России Алексея Мошкова каждую секунду 12 человек на Земле становятся жертвами киберпреступников. Это означает, что ежедневно количество пострадавших исчисляется сотнями тысяч, а ущерб может достигать миллиарды рублей [21].

Атаки на критически важные инфраструктуры, такие как энергетика и водоснабжение, действительно представляют серьезную угрозу для общества и экономики.

Основные последствия таких атак:

1. Отключение электроэнергии может привести к серьезным сбоям в работе городов, предприятий и даже целых регионов. Это затрагивает не только промышленность, но и повседневную жизнь граждан.

2. Взлом систем водоснабжения представляет опасность для здоровья населения, так как может привести к загрязнению воды или нарушению ее подачи.

3. Промышленное производство, особенно в таких секторах, как логистика и кораблестроение, также страдает от атак. Нарушение работы этих отраслей может парализовать цепочки поставок и нанести значительный экономический ущерб.

4. Микроэлектроника является важной отраслью, поскольку она связана с производством компонентов для различных устройств, включая те, которые используются в критической инфраструктуре. Атака на производителей микроэлектроники может повлиять на множество других секторов.

5. Производство продуктов питания и фармацевтическая промышленность играют ключевую роль в обеспечении базовых потребностей населения. Атаки на эти отрасли могут привести к дефициту жизненно важных товаров.

6. Добыча полезных ископаемых и металлургия также являются важными секторами, обеспечивающими сырьем различные производства. Нарушения в этих отраслях могут привести к перебоям в поставках сырья и материалов.

Для предотвращения подобных инцидентов необходимо уделять особое внимание кибербезопасности и внедрять современные технологии защиты информации. К таким мерам относятся:

– регулярное обновление программного обеспечения;

– использование современных средств защиты данных (антивирусы, межсетевые экраны);

– обучение сотрудников основам информационной безопасности;

– проведение регулярных аудитов и тестов на проникновение;

– разработка планов действий на случай чрезвычайных ситуаций.

Киберпреступность становится все более сложной задачей, требующей комплексного подхода со стороны государства, бизнеса и общества [51].

Обострение международной обстановки действительно оказывает значительное влияние на ландшафт киберугроз. В условиях геополитических напряженностей и конфликтов между государствами кибератаки становятся мощным инструментом воздействия на противника, и это особенно заметно в отношении объектов критической информационной инфраструктуры (КИИ).

КИИ включает в себя такие важные элементы, как энергетические сети, системы управления транспортом, здравоохранительные учреждения, финансовые институты и другие ключевые отрасли, от которых зависит нормальное функционирование государства и общества. Атаки на эти объекты могут иметь катастрофические последствия, начиная от перебоев в снабжении населения электроэнергией и водой до сбоев в системах здравоохранения и финансов. Рост числа атак с использованием методов взлома и вредоносного программного обеспечения свидетельствует о том, что злоумышленники стремятся максимально использовать уязвимости в системах безопасности. Эти атаки могут быть направлены как на кражу конфиденциальной информации, так и на нанесение прямого ущерба инфраструктуре, например, путем вывода из строя оборудования или манипуляций с данными [61].

Отметим, что в России предпринимаются активные усилия по укреплению информационной безопасности. Важным шагом в этом направлении стало подписание 12 апреля 2021 г. Указа Президента № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности». Этот документ определяет стратегический курс Российской Федерации на

международном уровне и нацелен на продвижение российской системы информационной безопасности, совершенствование взаимодействия между ведомствами внутри страны и участие в формировании международно-правовых механизмов урегулирования конфликтов в глобальном информационном пространстве [6].

Государственная политика в области обеспечения информационной безопасности детей и подростков основывается на конституционных гарантиях равенства прав и свобод граждан.

В 2023 году Распоряжением Правительства Российской Федерации от 28.04.2023 № 1105-р был утвержден документ «Об утверждении Концепции информационной безопасности детей в Российской Федерации и признании утратившим силу Распоряжения Правительства РФ от 02.12.2015 № 2471-р». Главная цель данной Концепции – защитить подрастающее поколение от информационных угроз и рисков в современной цифровой среде. В Концепции указывается, что «деструктивное информационное воздействие способствует развитию формирования у детей и подростков неправильного восприятия традиционных российских духовно-нравственных ценностей, провоцирующего «психологический слом», следствием которого могут стать как депрессивное состояние, так и проявление девиантного поведения, повышенной агрессии к окружающим»[5].

Стратегической целью государственной политики в области информационной безопасности подростков и детей является формирование безопасного информационного пространства.

Концепцией информационной безопасности детей в РФ были установлены приоритетные задачи государства, общественных и образовательных организаций, а именно «проведение мероприятий, направленных на повышение информационной грамотности детей и подростков, формирование навыков законопослушного и ответственного поведения в цифровой среде; совершенствование форм и методов

обеспечения информационной безопасности детей и подростков в соответствии с целями государственной политики по сохранению и укреплению традиционных ценностей; расширение спектра возможностей услуги «Родительский контроль» на стационарных и мобильных устройствах, которыми пользуется ребенок; развитие системы социальных и межличностных отношений и общения детей; развитие творческих способностей детей; воспитание у детей толерантности» [5].

В приоритете отмечена и работа со взрослым населением, здесь перспективными являются разработка и внедрение специальных образовательных и просветительских программ, содержащих информацию об информационных угрозах, о правилах безопасного пользования детьми сетью Интернет, средствах защиты несовершеннолетних от доступа к информации, наносящей вред их здоровью, нравственному и духовному развитию, предназначенных для родителей, работников системы образования, детских и юношеских библиотек и других специалистов, занятых обучением и воспитанием несовершеннолетних, организацией их досуга.

Таким образом, надлежащее выполнение обязанностей по осуществлению информационной защиты должно включать в себя перечень мер по контролю за поведением подрастающего поколения, мониторинг их деятельности и активности в информационно-телекоммуникационной сети Интернет, а также обучение и разъяснение правового использования коммуникациями.

Федеральный закон №124-ФЗ «Об основных гарантиях прав ребёнка в Российской Федерации» включает меры по защите детей от вредной для их здоровья и развития информации, причем «ребенок - лицо до достижения им возраста 18 лет (совершеннолетия)» [9].

В частности, статья 14 этого закона посвящена вопросам защиты подрастающего поколения от информации, пропаганды и агитации, наносящих вред его здоровью, нравственному и духовному развитию.

В законе прописаны обязанности органов государственной власти, местного самоуправления, юридических лиц и граждан, направленные на предотвращение распространения такой информации среди несовершеннолетних. Кроме того, в статье 5 данного закона указывается, что государство обязано обеспечивать защиту детей и подростков от факторов, негативно влияющих на его физическое, интеллектуальное, психическое, духовное и нравственное развитие. Это касается как средств массовой информации, так и других источников информации, которые могут оказывать негативное воздействие на них. Таким образом, этот закон направлен на создание условий, при которых дети и подростки будут защищены от вредоносного контента и смогут развиваться в безопасной информационной среде [9].

Повышение информационной и медиаграмотности обучающихся определяется как задача государства и образовательных организаций. Подрастающее поколение должно с раннего возраста приобретать навыки безопасного существования в современном информационном пространстве. Причем возрастно-психологический подход к оценке вредного воздействия информационной продукции на психическое развитие, здоровье и психологическое благополучие детей, который лег в основу Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию», показал свою достаточно высокую эффективность[12].

В Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы указано, что «Для формирования информационного пространства знаний необходимо:

а) проводить мероприятия в области духовно-нравственного воспитания граждан;

б) реализовать просветительские проекты, направленные на обеспечение доступа к знаниям, достижениям современной науки и культуры;

в) проводить мероприятия по сохранению культуры и общероссийской идентичности народов Российской Федерации;

г) сформировать безопасную информационную среду на основе популяризации информационных ресурсов, способствующих распространению традиционных российских духовно-нравственных ценностей;

д) усовершенствовать механизмы обмена знаниями;

ж) обеспечить условия для научно-технического творчества, включая создание площадок для самореализации представителей образовательных и научных организаций;

з) обеспечить совершенствование дополнительного образования для привлечения детей к занятиям научными изысканиями и творчеством, развития их способности решать нестандартные задачи;

и) использовать и развивать различные образовательные технологии, в том числе дистанционные, электронное обучение, при реализации образовательных программ…» [8].

Преобразования, происходящие в российском обществе и экономике, влияют и на сферу профессионального образования, ориентируя ее на привлечение инновационных цифровых технологий для интенсификации процесса формирования профессиональных навыков студентов. Современная политика в сфере среднего профессионального образования диктует условия развития образовательного сообщества, ориентируясь на запросы будущих работодателей и модернизируя существующие формы подготовки выпускников профессиональных образовательных организаций, независимо от возможных сфер профессиональной деятельности.

Особый интерес представляют профессиональные образовательные организации среднего профессионального образования, непосредственно задействованные в федеральном проекте «Профессионалитет». ГБПОУ «ЮУрГТК» реализует с 2022 года ФП Профессионалитет [56].

Федеральный проект «Профессионалитет» — это федеральная программа, направленная на модернизацию системы среднего профессионального образования (СПО) в России. Цель проекта — подготовить высококвалифицированных специалистов для приоритетных отраслей экономики страны, таких как машиностроение, металлургия, сельское хозяйство, строительство и другие. Проект реализуется Министерством просвещения Российской Федерации совместно с крупными предприятиями и отраслевыми объединениями.

Ключевые аспекты проекта «Профессионалитет»:

1. Интеграция образования и производства. Образование становится более прикладным и ориентированным на конкретные производственные процессы. Учащиеся проходят практику непосредственно на предприятиях, что позволяет им приобрести реальные навыки и опыт работы.

2. Модернизация материально-технической базы. Создаются новые учебные центры и мастерские, оснащённые современным оборудованием, соответствующими реальным условиям труда на производстве.

3. Повышение квалификации преподавателей. Преподаватели образовательных организаций проходят дополнительное обучение и стажировки на предприятиях, чтобы быть в курсе последних тенденций и технологий в отрасли.

4. Развитие дуального образования. Дуальное образование сочетает теоретическое обучение в колледже с практикой на предприятии. Это позволяет студентам одновременно получать знания и опыт работы.

5. Создание кластеров. Формирование отраслевых образовательных кластеров, объединяющих колледжи, предприятия и научные институты. Это способствует эффективному обмену знаниями и технологиями.

6. Внедрение новых образовательных стандартов. Разработка и внедрение новых образовательных стандартов, соответствующих современным требованиям рынка труда и международным стандартам.

7. Содействие трудоустройству выпускников. Активное сотрудничество с работодателями для обеспечения трудоустройства выпускников после окончания обучения [16].

Проект «Профессионалитет» призван повысить конкурентоспособность российской промышленности и обеспечить экономику страны квалифицированными кадрами.

Информация о предложенных вакансиях с онлайн-сервисов и платформ для поиска работы позволяет заключить, что около 92% работодателей заинтересованы в потенциальных сотрудниках, владеющих такими гибкими навыками, как информационная грамотность, активное обучение, умение вести переговоры, адаптивность, навыки тайм-менеджмента, работа в команде.

Необходимость решения проблемы формирования цифровых навыков студентов профессиональных образовательных организаций отражены в таких нормативно-правовых актах Российской Федерации, как федеральные проекты «Молодые профессионалы» и «Цифровая образовательная среда». В этих документах формирование цифровых навыков выступает одним из ключевых направлений образования. Федеральный проект «Молодые профессионалы» нацелен на повышение конкурентоспособности профессионального образования [15].

В федеральном проекте «Цифровая образовательная среда» подчеркивается необходимость создания и внедрения в образовательных организациях цифровой образовательной среды и обеспечения реализации цифровой трансформации системы образования [17]. Оба национальных проекта взаимосвязаны, они обусловливают актуальность исследования – формирование гибких и профессиональных навыков студентов в цифровой образовательной среде профессиональной образовательной организации.

Подростковый возраст – это время активного формирования личности, когда молодые люди начинают проявлять интерес к новым технологиям и возможностям интернета.

Однако вместе с этим возрастает риск столкнуться с угрозами в цифровой среде. Поэтому важно уделять особое внимание вопросам информационной и кибербезопасности в образовательных организациях.

Примерная основная образовательная программа среднего общего образования подчеркивает важность обучения студентов профессиональных образовательных организаций компетенциям в сфере информационной безопасности. Например, целью изучения общеобразовательной учебной дисциплины «Информатика» является подготовка выпускников к успешной адаптации и эффективной работе в условиях современного информационного общества. Сегодня информационные компетенции играют ключевую роль практически в любой профессиональной деятельности, независимо от выбранной специальности. Они включают в себя умение работать с различными цифровыми инструментами, обрабатывать информацию, решать задачи с помощью компьютерных технологий и обеспечивать безопасность данных [45].

В требованиях к предметным результатам освоения базового курса информатики, одним из пунктов является понимание угроз информационной безопасности, использование методов и средств противодействия этим угрозам, соблюдение мер безопасности, предотвращающих незаконное распространение персональных данных; соблюдение требований техники безопасности и гигиены при работе с компьютерами и другими компонентами цифрового окружения; понимание правовых основ использования компьютерных программ, баз данных и работы в сети Интернет.

Наиболее очевидной является возможность дополнения вопросами кибербезопасности уроков информатики, однако можно включить модули по кибербезопасности и в другие учебные дисциплины, например, такие как Основы безопасности жизнедеятельности и защиты Родины, Русский

язык, Обществознание, История и Литература, причем не только общеобразовательные.

Таким образом, интеграция вопросов кибербезопасности в учебные дисциплины позволило бы создать целостное представление у студентов об этой важной теме и помогло бы сформировать у них навыки безопасного поведения в цифровом мире.

Кибербезопасность стала неотъемлемой частью нашей жизни, и образовательные учреждения не являются исключением. Информационные технологии используются повсеместно, начиная от проведения лекций и семинаров до хранения и обмена учебными материалами. Следовательно, каждый участник образовательного процесса: будь то студент, преподаватель или администратор или родитель – подвержен различным киберугрозам. Спам, вирусы, взлом компьютеров и другие виды атак могут не только нарушить учебный процесс, но и поставить под угрозу личные данные участников. Важно, чтобы все понимали, как минимизировать эти риски и как правильно реагировать на инциденты.

Интеграция вопросов кибербезопасности в образовательный процесс – это шаг к созданию более защищенной среды обучения и воспитания ответственного отношения к использованию информационных технологий.

1.2 Сущность основных понятий кибербезопасности

В Федеральном законе от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» было указано, что защита информации включает комплекс мероприятий, которые направлены на предотвращение несанкционированного доступа к данным, их утраты, изменения или раскрытия без разрешения. В рамках этого процесса важно обеспечить конфиденциальность (защиту от несанкционированного доступа), целостность (предотвращение изменений данных без разрешения) и доступность (гарантирование того, что информация будет доступна авторизованным пользователям тогда, когда

это необходимо). Кроме того, защита информации может включать правовые меры (например, законодательные акты о защите персональных данных), организационные меры (разработка политик безопасности внутри организации) и технические меры (использование шифрования, антивирусных программ и других средств защиты) [10].

Однако в данном законе не сформулированы понятия информационная безопасность и кибербезопасность. Закон также не затрагивает вопросы, касающиеся обеспечения безопасности граждан и подрастающего поколения в сети Интернет.

Термин «кибербезопасность» (cybersecurity) получил распространение в середине 1990-х гг. сначала в США, затем в Европе, а позднее – и в других странах [49].

Слово «кибербезопасность» происходит от греческого слова κυβερνητικός и означает искусство управления. Данный термин действительно широко используется в средствах массовой информации и публичных дискуссиях, связанных с защитой информации и противодействием киберугрозам. Однако в научной литературе термин применяется реже, чем в популярной прессе и аналитических отчетах.

В то же время в большинстве зарубежных стран толкование понятия кибербезопасность выделяется в самостоятельное определение. Так Национальный институт стандартов и технологий США (NIST) дает определение кибербезопасности как «способность защищать или защищать использование киберпространства от кибератак» [60].

В ISO/IEC 27032:2023(en) Cybersecurity — Guidelines for Internet security, было отмечено, что «cybersecurity –safeguarding of people, society, organizations and nations from cyber risks», т.е. кибербезопасность – защита людей, общества, организаций и стран от киберрисков [58].

В ноябре 2013 года в Совете Федерации прошли парламентские слушания по вопросам кибербезопасности, где обсуждалась концепция стратегии кибербезопасности Российской Федерации. Признав

актуальность угроз информационной безопасности, и в частности, кибербезопасности, личности, организациям и государству, участники слушаний предложили вынести на обсуждение в Интернете проект Концепции стратегии кибербезопасности Российской Федерации. Участники слушаний подчеркнули важность защиты информации, как для граждан, так и для организаций и государства в целом.

В проекте Концепции стратегии кибербезопасности Российской Федерации было отмечено, что киберпространство – это «сфера деятельности в информационном пространстве, образованная совокупностью Интернета и других телекоммуникационных сетей и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)», а кибербезопасность – как «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями» [3].

ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели, указывает, что «кибербезопасность (киберзащита) (cybersecurity): Действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли, или повреждения критических систем или информационных объектов. Примечание – Цель при этом – уменьшить персональный риск травмирования или риск угрозы здоровью населения, риск потери доверия общественности или потребителей, разглашения информации о важных объектах, незащищенности бизнес-объектов или несоответствия нормативам. Эти понятия применимы к любой системе в производственном процессе, которая может включать в себя как независимые, так и связанные компоненты. Коммуникация между системами может осуществляться либо с помощью внутренних

сообщений, либо через любые пользовательские или машинные интерфейсы, которые обеспечивают аутентификацию, работу, управление или обмен данными с любой из таких систем управления. Кибербезопасность включает в себя понятия идентификации, аутентификации, отслеживаемости, авторизации, доступности и приватности»[19].

Кибербезопасность представляет собой область, связанную с защитой компьютерных систем, сетевой инфраструктуры, устройств Интернета вещей и других цифровых активов от несанкционированного доступа, повреждения, сбоев, утечки данных и прочих киберугроз. Включает методы, технологии и процессы, направленные на выявление, предотвращение, обнаружение и реагирование на киберинциденты.

Кибербезопасность критически важна для обеспечения конфиденциальности, целостности и доступности информации в условиях растущей взаимосвязанности и зависимости от информационных технологий.

Целью кибербезопасности является непрерывная защита сетевых систем и данных от несанкционированного доступа.

Кибербезопасность – это защита компьютерных систем и сетей от несанкционированного доступа, взлома и других угроз в цифровом пространстве. Представьте, что ваш компьютер или смартфон могут подвергнуться атаке хакеров, которые пытаются получить доступ к личным данным или заблокировать работу устройства. Кибербезопасность – это «броня», которая защищает твои устройства и информацию от таких киберугроз с помощью антивирусов, брандмауэров и других мер.

Основные направления кибербезопасности:

1) Безопасность приложений. Разработка и тестирование программного обеспечения с учетом требований безопасности. Включает анализ кода на наличие уязвимостей, использование безопасных методов разработки и регулярные обновления программного обеспечения.

2) Защита данных. Обеспечение конфиденциальности, целостности и доступности информации. Защита данных включает шифрование данных, управление доступом, резервное копирование и восстановление данных.

3) Инцидент-менеджмент и реагирование на инциденты. Планирование и реализация мер по обнаружению, расследованию и устранению последствий инцидентов в сфере кибербезопасности. Включает создание планов действий при чрезвычайных ситуациях и проведение регулярных учений.

4) Мобильная безопасность. Защита мобильных устройств и приложений от угроз, связанных с их использованием. Включает антивирусные программы, контроль над установкой приложений и системы управления мобильными устройствами.

5) Облачная безопасность. Обеспечение безопасности данных и приложений, размещенных в облачных сервисах. Направление включает защиту виртуальных машин и микросервисов, а также мониторинг активности в облаке.

6) Обучение и повышение осведомленности. Повышение уровня знаний сотрудников и пользователей о принципах кибербезопасности. Включает тренинги, симуляции фишинговых атак и другие мероприятия.

7) Сетевая безопасность. Защита сетевой инфраструктуры от атак, таких как DDoS, взломы и перехват трафика. Сетевую безопасность обеспечивают брандмауэры, системы обнаружения и предотвращения вторжений.

8) Соответствие требованиям регуляторов и стандартам безопасности. Соблюдение нормативных актов и стандартов в области кибербезопасности, таких как ISO/IEC 27001 и другие.

9) Управление идентификацией и доступом. Обеспечивает контроль за теми, кто имеет доступ к различным ресурсам и данным. Включает аутентификацию пользователей, авторизацию, управление учетными записями и ролями.

10) Криптография. Использование криптографических методов для защиты данных, включая алгоритмы шифрования, цифровые подписи и хеш-функции. [31].

Компания Microsoft отмечает, что кибербезопасность – комплексный подход, который объединяет три ключевых компонента: людей, процессы и технологии. «Кибербезопасность – это набор процессов, передовых практик и технологий, которые помогают защитить критически важные системы и сети от цифровых атак» [42].

Специалисты Лаборатории Касперского указывают, что кибербезопасность – это «совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных» [54].

В источнике ИСО/МЭК 27032:2023 Cybersecurity – Guidelines for Internet security «Руководство по безопасности в Интернете» было указано, что «кибербезопасность – условия защищенности от физических, духовных, финансовых, политических, эмоциональных, профессиональных, психологических, образовательных или других типов воздействий или последствий аварии, повреждения, ошибки, несчастного случая, вреда или любого другого события в киберпространстве, которые могли бы считаться нежелательными» [58].

Такое широкое понимание кибербезопасности подчеркивает необходимость комплексного подхода к защите информации и систем, учитывая не только технические аспекты, но и влияние на жизнь и благополучие людей. В исследованиях, связанных с обеспечением защиты используемых данных, понятия «кибербезопасность» и «информационная безопасность» часто используются как синонимы. Однако это не так.

Информационная безопасность связана с обеспечением безопасности данных в любой форме (цифровой или аналоговой) и является немного более широким понятием, чем кибербезопасность. Кибербезопасность это часть информационной безопасности.

Информационная безопасность действительно выступает своего рода «зонтом», охватывающим различные аспекты защиты информации. Под этим зонтом находятся более узкие направления, такие как:

– кибербезопасность – защита информационных систем от несанкционированного доступа, изменений данных, атак злоумышленников и других угроз, связанных с использованием компьютерных сетей;

– криптография – методы шифрования и дешифровки данных для обеспечения конфиденциальности и целостности информации при передаче и хранении;

– безопасность мобильных устройств – меры по защите мобильных телефонов, планшетов и других портативных устройств от взлома, утечек данных и вредоносных программ;

– физическая безопасность – обеспечение физической защиты серверов, центров обработки данных и другой инфраструктуры;

– управление доступом – контроль за тем, кто имеет право доступа к различным ресурсам системы;

– аудит и мониторинг – регулярное отслеживание состояния информационной безопасности и выявление потенциальных уязвимостей.

Таким образом, ИБ охватывает широкий спектр мер и технологий, направленных на защиту информации во всех её формах и средах [24].

Бизнес, связанный с ИБ имеет основную задачу защитить данные коммерческой компании от несанкционированного доступа любого рода. Бизнес, связанный с кибербезопасностью, имеет основную задачу обеспечения защиты данных компании от несанкционированного электронного доступа. Но, в любом случае, цель информационной безопасности и кибербезопасности это защита данных [34].

Таким образом, кибербезопасность является частью ИБ и обеспечивает защиту приложений, сетевую безопасность, интернет-безопасность объектов особо важной информационной инфраструктуры.

Выводы по первой главе

Первая глава вашего текста охватывает важные теоретические аспекты, связанные с формированием основ кибербезопасности. В этой части работы рассматриваются следующие ключевые моменты:

1. Современное состояние проблемы кибербезопасности – здесь анализируются текущие вызовы и угрозы в области информационной безопасности; разъяснена роль государства и образовательных организаций в решении данных проблем.

2. Сущность основных понятий кибербезопасности – этот раздел посвящен разъяснению ключевого термина кибербезопасность, разъясняется цель кибербезопасности, основные направления и отличие кибербезопасности от информационной безопасности.

Таким образом, первая глава закладывает фундамент для дальнейшего изучения вопросов кибербезопасности в контексте профессионального образования.

Резюмируя все вышесказанное, можно сказать, что кибербезопасность – это область знаний и практики, направленная на защиту компьютерных систем, сетей, устройств и данных от различных видов цифровых угроз. Она охватывает широкий спектр методов и технологий для предотвращения, обнаружения и реагирования на кибератаки, а также восстановления после них.

ГЛАВА 2. ФОРМИРОВАНИЕ ОСНОВ КИБЕРБЕЗОПАСНОСТИ У ОБУЧАЮЩИХСЯ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ ПРИ ПРЕПОДАВАНИИ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ДИСЦИПЛИНЫ ИНФОРМАТИКА

2.1 Информационная среда ГБПОУ «Южно-Уральский государственный технический колледж» как фактор формирования основ кибербезопасности у студентов профессиональной образовательной организации

В Федеральном законе «Об образовании» указано, что «профессиональная образовательная организация (ПОО) – образовательная организация, осуществляющая в качестве основной цели ее деятельности образовательную деятельность по образовательным программам среднего профессионального образования и (или) по программам профессионального обучения;….обучающийся – физическое лицо, осваивающее образовательную программу» [13].

Исследование проблемы формирования кибербезопасности студентов ПОО проходило в Государственном бюджетном профессиональном образовательном учреждении «Южно-Уральский государственный технический колледж» (ГБПОУ «ЮУрГТК»), в котором на сегодняшний день обучаются около 3000 студентов.

ГБПОУ «ЮУрГТК» находится под управлением Министерства образования и науки Челябинской области. В колледже работают 173 преподавателя, что говорит о достаточно большом штате педагогов.

Преподаватели обладают как практическим опытом работы по своей специальности, так и глубокой теоретической подготовкой. Это важно для качественной реализации образовательных программ. Среди личного состава организации есть кандидаты наук, заслуженные работники образования Российской Федерации и преподаватели высшей квалификационной категории.

Колледж предлагает обучение по 45 программам подготовки специалистов среднего звена. Обучение возможно как на бюджетной, так и на коммерческой основе. ЮУрГТК представляет собой учебное заведение с квалифицированным преподавательским составом и широким спектром образовательных программ.

Директор колледжа Тубер Игорь Иосифович – заслуженный учитель РФ, кандидат педагогических наук, почетный строитель России, председатель совета директоров ПОО Челябинской области, член совета директоров ВУЗов Челябинской области, член коллегии Министерства образования и науки Челябинской области, председатель правления Ассоциации образовательных учреждений СПО Челябинской области [56].

Организационная структура управления ГБПОУ «Южно-Уральский государственный технический колледж» представлена на рисунке 1.

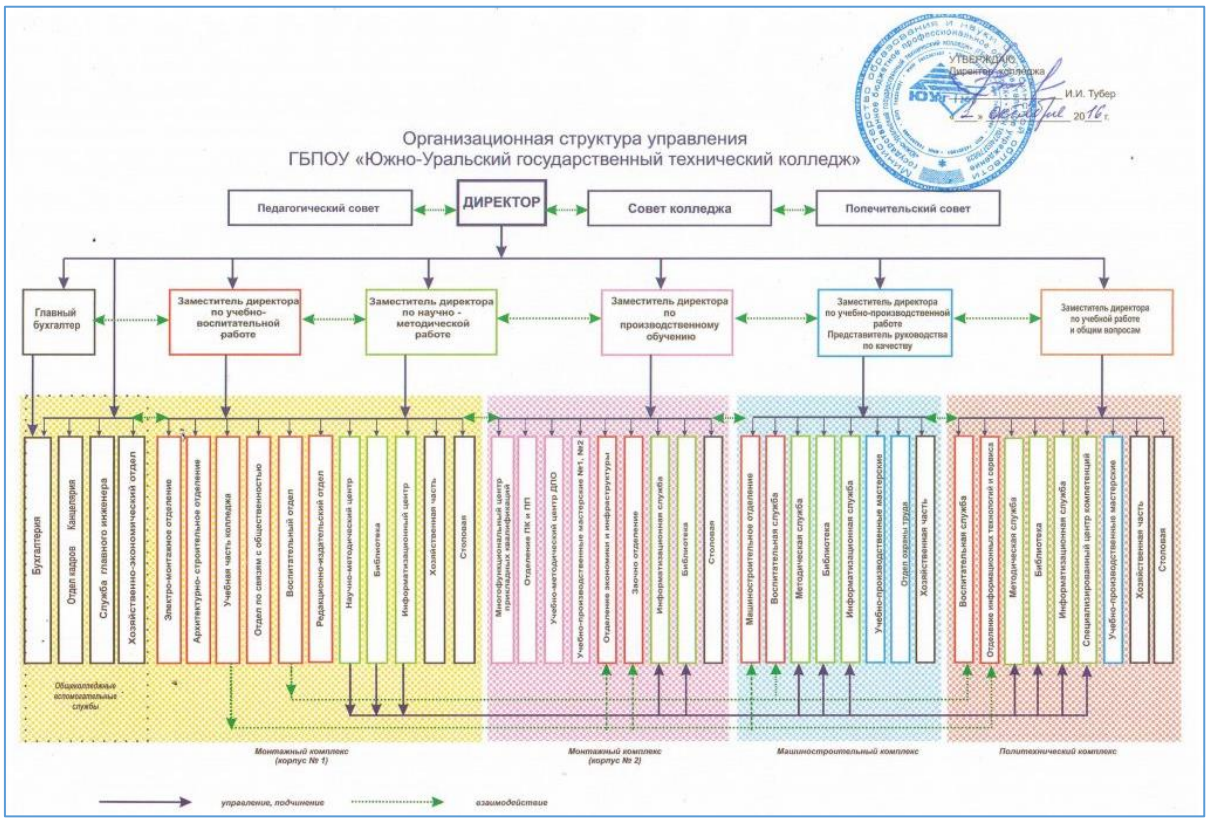

Рисунок 1 – Организационная структура управления ГБПОУ «ЮУрГТК»

Структурное подразделение, отвечающее за состояние единой информационной среды колледжа – информатизационный центр.

Цифровая информационно-образовательная среда образовательного учреждения – это:

– Информационная открытость. Обеспечивает соответствие требованиям законодательства Российской Федерации в сфере образования, касающихся прозрачности деятельности учебного заведения. Это включает публикацию необходимых данных об учреждении, его программах, результатах работы, финансовом состоянии и других аспектах, которые должны быть доступны общественности согласно законодательству.

1) Применение современных технологий в обучении. Этот пункт касается внедрения электронных форматов обучения и использования цифровых технологий в образовательном процессе. Включает организацию учебных занятий, проведение оценочных мероприятий и использование дистанционных образовательных технологий при реализации программ среднего профессионального и дополнительного образования. Важно отметить, что это предполагает применение различных информационных ресурсов и сервисов, обеспечивающих цифровое взаимодействие между студентами, преподавателями и самой образовательной средой.

2) Индивидуализация образовательной траектории. Этот пункт подчеркивает важность создания условий для того, чтобы каждый студент мог выбирать свою собственную траекторию обучения. Индивидуальный подход позволяет учитывать личные интересы, способности и потребности обучающихся, а также адаптировать учебный процесс таким образом, чтобы он максимально соответствовал целям каждого студента. Это может включать выбор дополнительных дисциплин, участие в проектах и другие формы индивидуального подхода.

3) Удаленный доступ к информационным ресурсам и электронным учебным курсам. Данный пункт акцентирует внимание на необходимости обеспечения всем участникам образовательного процесса (студентам,

слушателям курсов, преподавателям) возможности доступа к необходимым материалам и сервисам независимо от их физического местоположения. Это особенно актуально в условиях дистанционного обучения, когда студенты могут находиться за пределами учебного заведения или даже региона. Доступ к цифровым библиотекам, электронным учебникам, онлайн-курсам и другим образовательным ресурсам должен быть организован таким образом, чтобы участники могли эффективно использовать эти материалы в любое время и из любой точки мира.

4) Реализация механизмов и процедур мониторинга качества образовательного процесса. Мониторинг качества образовательного процесса подразумевает регулярную оценку эффективности учебной деятельности, включая анализ успеваемости студентов, работу преподавателей, качество учебных материалов и методов обучения. Для этого используются различные инструменты и процедуры, такие как тестирование, опросы, анализ обратной связи от студентов и преподавателей, оценка достижений студентов по итогам семестров и т.д. Мониторинг помогает выявить слабые стороны и своевременно внести коррективы в образовательный процесс, обеспечивая его высокое качество.

5) Обеспечение доступной образовательной среды. Создание доступной образовательной среды означает, что все участники образовательного процесса, независимо от своих физических возможностей, должны иметь равные условия для получения знаний. Это включает адаптацию учебных помещений, оборудования и учебных материалов для людей с ограниченными возможностями здоровья (ОВЗ), а также внедрение специальных технологий и методик обучения, которые позволяют каждому учащемуся участвовать в учебном процессе наравне со всеми. Доступная среда способствует инклюзивности и делает образование доступным для всех категорий граждан.

Все это направлено на повышение качества образовательного процесса и обеспечение соответствия современным стандартам и требованиям в образовании.

Цифровая информационно-образовательная среда профессиональной образовательной организации (ЦИОС) — это комплекс взаимосвязанных компонентов, включающий в себя:

1. Электронные информационные и образовательные ресурсы:

– онлайн-платформы для взаимодействия студентов и преподавателей, такие как системы управления обучением и Сферум;

– учебники, методические пособия, лекции, презентации и другие учебные материалы в электронном формате;

– электронные библиотеки, базы данных, архивы научных статей и публикаций.

2. Совокупность информационных и телекоммуникационных технологий:

– программное обеспечение для дистанционного обучения, видеоконференцсвязь, системы тестирования и контроля знаний;

– системы автоматизации учебного процесса, такие как планирование расписания, учет посещаемости и успеваемости;

– средства для разработки и размещения электронных учебных курсов.

3. Технологические средства:

– компьютеры, планшеты, смартфоны и другие устройства, позволяющие студентам и преподавателям взаимодействовать с ЦИОС;

– серверы, хранилища данных, сетевое оборудование, необходимое для функционирования всей инфраструктуры.

Целью информационно-образовательной среды является предоставление возможности студентам осваивать образовательные программы независимо от их географического положения.

ЦИОС обеспечивает доступность образования, позволяя обучающимся получать знания и навыки через интернет, используя современные технологии и ресурсы, функционирование которой регламентируется локальным нормативным актом – СМК-ПП-126-02 Положение о цифровой информационно-образовательной среде.

В колледже существует система дистанционного обучения (СДО), специализированный веб-сайт dom.sustec.ru, который предназначен для организации электронного обучения и обучения с применением дистанционных образовательных технологий. Сайт разработан на основе системы управления образовательными электронными курсами Moodle и вход на сайт осуществляется для авторизованных пользователей [48].

Основные особенности СДО:

1) Авторизация пользователей. Доступ к системе возможен только для зарегистрированных пользователей. Это гарантирует безопасность данных и ограничивает доступ к образовательному контенту исключительно для студентов и преподавателей колледжа.

2) Логины и пароли. Каждому студенту, поступившему в учебное заведение, предоставляется индивидуальный логин и пароль для входа на портал СДО. Это обеспечивает персонализированный доступ к учебным материалам и возможность отслеживать прогресс обучения.

3) Функциональность портала. Портал СДО позволяет студентам: получать доступ к электронным учебным материалам (лекциям, заданиям, тестам и др.); участвовать в дистанционных занятиях и олимпиадах; общаться с преподавателями и другими студентами через встроенные коммуникационные инструменты (форумы, чаты и т.п.); проходить контрольные мероприятия (тестирования, экзамены) в режиме онлайн [59].

Использование такой системы значительно упрощает процесс обучения, особенно в условиях невозможности личного присутствия на занятиях, например, во время карантина или болезни или для студентов, проживающих вдали от учебного заведения.

Реализация функции электронного дневника/журнала в колледже осуществляется через ГИС «Сетевой город. Образование», которая значительно упрощает управление процессом обучения, повышает прозрачность и доступность информации для всех участников образовательного процесса. Вход в электронный журнал АИС «Сетевой город. Образование» по ссылке https://poo.edu-74.ru/.

Приобретение доступа к электронным учебным изданиям через электронную библиотечную систему (ЭБС) «Знаниум» является значительным шагом в обеспечении качественного образовательного процесса [56].

Преимущества приобретения доступа к ЭБС:

1) Доступность учебных материалов. Студенты получают круглосуточный доступ к обширной базе учебных изданий, что позволяет им изучать материал в удобное для них время и месте.

2) Актуальность контента. Электронные издания часто обновляются быстрее, чем печатные аналоги, что обеспечивает актуальность предоставляемых знаний.

3) Экономия ресурсов. Покупка доступа к ЭБС обходится дешевле, чем приобретение большого количества бумажных книг, особенно если учесть затраты на хранение и обновление фондов.

4) Удобство поиска и навигации. Современные ЭБС предлагают удобные инструменты для поиска нужной информации, что экономит время и облегчает процесс изучения.

5) Экологичность. Использование электронных ресурсов снижает потребление бумаги и уменьшает углеродный след образовательного учреждения.

Возможности использования ЭБС:

1) Интерактивные элементы. Многие электронные учебники содержат мультимедийные компоненты (видео, аудио, тесты), что делает процесс обучения более интересным и эффективным.

2) Возможность интеграции с другими системами. ЭБС могут быть интегрированы с системами дистанционного обучения, что позволяет преподавателям легко добавлять ссылки на нужные материалы прямо в учебные курсы.

3) Анализ статистики использования. Администраторы и преподаватели могут отслеживать, какие материалы наиболее востребованы среди студентов, что помогает оптимизировать подбор литературы [55].

Организация работы с ЭБС:

1) Регистрация и доступ. Студенты и преподаватели получают индивидуальные логины и пароли для доступа к системе. Обычно доступ предоставляется на определенный срок (например, на весь период обучения).

2) Инструктаж и обучение. Проводится обучение студентов и преподавателей работе с ЭБС, объяснить, как искать нужную литературу, скачивать документы и пользоваться дополнительными функциями.

3) Техподдержка. Обеспечивается техническая поддержка, чтобы пользователи могли быстро решать возникающие проблемы.

Приобретение доступа к ЭБС существенно улучшает образовательный процесс, делая его более гибким, доступным и эффективным. Это шаг вперед в использовании современных технологий для повышения качества образования.

Доступ к сети Интернет. В колледже обеспечен доступ к сети Интернет с любого ПК (при условии авторизованного входа в локальную сеть колледжа).

Доступ к электронным образовательным ресурсам. Все студенты колледжа имеют доступ к электронным образовательным ресурсам и профессиональным базам данных, размещенных в подразделе Белый список сайтов по ссылке https://sustec.ru/studentu/belyy-spisok-saytov/ и

систематизированных по общеобразовательным дисциплинам, циклам ЕН, ОГСЭ, СГЦ и специальностям.

Учебное заведение действительно располагает значительной учебно-материальной базой, которая позволяет качественно осуществлять образовательный процесс [56]. Рассмотрим подробнее структуру и состав учебно-материальной базы:

1) Объекты недвижимости:

– общее количество объектов: 56,

– общая площадь: 59 596 кв. м.

2) Инфраструктура:

– учебные корпуса: 4,

– стадионы: 2,

– лыжная база: 1,

– спортивные площадки: 2,

– спортивные залы: 5,

– учебно-производственные мастерские: 9,

– учебные полигоны: 3,

– библиотеки: 4.

3) Учебные помещения:

– кабинеты по общеобразовательным дисциплинам и дисциплинам циклов ОГСЭ и ЕН: 36,

– кабинеты профессионального цикла: 80,

– учебные лаборатории: 55,

– компьютерные классы: 30,

– аудитории, оснащенные интерактивными досками или мультимедийными установками: 25.

В колледже имеются необходимые объекты для организации физкультурно-массовой и спортивно-оздоровительной работы: 2 спортивные площадки; лыжная база; 5 спортивных залов; 1 тренажерный

зал. Объекты для организации физкультурно-массовой и спортивно-оздоровительной работы имеются в каждом из учебных корпусов. Наличие спортивных сооружений и площадок способствует развитию физической культуры и активного образа жизни студентов.

Учебные полигоны и мастерские предоставляют возможность для практических занятий и отработки профессиональных навыков. Оснащенность учебно-производственных мастерских и полигонов необходимым оборудованием, инструментами и материалами играет ключевую роль в подготовке высококвалифицированных специалистов, а библиотеки учебного заведения обеспечивают доступ к необходимой литературе и информационным ресурсам. Эта инфраструктура позволяет обеспечивать качественное образование по специальностям СПО.

Наличие специальных технических средств обучения для инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) свидетельствует о том, что колледж уделяет особое внимание созданию доступной и инклюзивной образовательной среды. Такие средства помогают обеспечить равные возможности для всех студентов, независимо от их физических особенностей.

На территории Машиностроительного комплекса колледжа имеются подъездные пандусы с поручнем ко входу в колледж и отдельное место для парковки автотранспортных средств инвалидов. В здании комплекса для лиц с нарушением опорно-двигательного аппарат есть доступный вход и возможность беспрепятственного доступа студентов в учебную аудиторию, библиотеку, санитарную комнату, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и других специальных приспособлений); имеются средства информационно-навигационной поддержки; сигнальные кнопки – вызов. Специализированные аудитории и помещения колледжа оборудованы в соответствии с требованиями СНиП и ГОСТ.

Применение системы дистанционного обучения Moodle на сайте dom.sustec.ru играет важную роль в повышении качества и доступности образовательного процесса. Moodle — это популярная платформа для организации электронного обучения, которая предоставляет широкий спектр инструментов для создания и управления учебными курсами, проведения тестов и экзаменов, общения между студентами и преподавателями, а также отслеживания прогресса обучения [59].

Таким образом, сочетание специальных технических средств для инвалидов и лиц с ограниченными возможностями здоровья с использованием современной системы дистанционного обучения Moodle позволяет колледжу создать комфортные условия для обучения всех студентов, обеспечивая высокий уровень доступности и качества образования.

Организация медицинского обслуживания и создание здоровьесберегающей среды являются важными аспектами деятельности любого образовательного учреждения.

В данном случае, колледж уделяет серьезное внимание здоровью студентов, что подтверждается наличием достаточного количества медицинских пунктов и проведением лечебно-оздоровительной работы.

1) Медицинское обслуживание. Колледж располагает двумя медицинскими пунктами, что позволяет охватить большую часть студенческого контингента. Один медицинский пункт расположен на территории Монтажного комплекса, другой на территории Политехнического комплекса. Такое распределение позволяет обеспечить быстрый доступ к медицинской помощи для студентов, находящихся в разных частях колледжа.

2) Лечебно–оздоровительная работа. Проведение плановой лечебно-оздоровительной работы включает в себя профилактику заболеваний, мониторинг состояния здоровья студентов, а также оказание первой

медицинской помощи при необходимости. Это важный элемент поддержания здоровья и предотвращения возможных осложнений.

Здоровьесберегающая среда профессиональной образовательной организации ГБПОУ «ЮУрГТК»:

1) Материальная база. Наличие достаточного количества медицинских кабинетов и оборудования свидетельствует о готовности колледжа оперативно реагировать на любые медицинские ситуации и оказывать необходимую помощь.

2) Доступность услуг. Расположение медицинских пунктов на территориях различных комплексов колледжа обеспечивает удобство и оперативность обращения за медицинской помощью.

3) Комплексный подход. Плановая лечебно-оздоровительная работа направлена на поддержание общего здоровья студентов, что способствует улучшению их самочувствия и повышению успеваемости.

Таким образом, наличие развитой медицинской инфраструктуры и систематическая работа по поддержанию здоровья студентов создают благоприятные условия для учебы и развития, способствуя сохранению и укреплению здоровья обучающихся.

Библиотека колледжа играет ведущую роль в обеспечении образовательного процесса источниками учебной информации. Рассмотрим её характеристики: количество библиотек: 4 (во всех комплексах колледжа); общая площадь 1128 кв. м; посадочные места в читальных залах 214 [56].

Структура и оснащение библиотеки учебного заведения:

1) Автоматизированная зона для самостоятельной работы студентов. Эта зона в библиотеке монтажного комплекса позволяет студентам самостоятельно заниматься, пользуясь современными техническими средствами.

2) Рабочие места библиотекарей. Все рабочие места библиотекарей автоматизированы, что ускоряет обработку запросов и поиск информации.

3) Оборудование. Библиотека оснащена принтерами, сканерами и копировальной техникой, что позволяет студентам, сотрудникам и преподавателям пользоваться различными услугами.

4) В библиотеках всех комплексов внедрена автоматизированная информационно-библиотечная система 1С: Библиотека, которая позволила решить задачу сплошной компьютеризации библиотек, начиная от ввода библиографической записи в электронный каталог до использования технологии электронной книговыдачи.

Фонд библиотеки: общий библиотечный фонд 143 838 экземпляров; электронные учебники 8 862 экземпляра; помимо учебной литературы, фонд включает официальные, справочно-библиографические, нормативно-технические, научные и художественные издания. Библиотечный фонд постоянно пополняется.

Роль библиотеки в образовательном процессе:

1) Доступ к учебной информации. Библиотека предоставляет студентам и преподавателям доступ к широкому спектру учебной литературы, что способствует качественному обучению и исследовательской деятельности.

2) Самостоятельная работа. Автоматизированная зона и читальные залы позволяют студентам проводить самостоятельные исследования, готовиться к занятиям и экзаменам.

3) Современные технологии. Использование электронных учебников и автоматизированных рабочих мест библиотекарей делает процесс поиска и получения информации более быстрым и удобным.

4) Разнообразие источников. Наличие официальных, справочно-библиографических, научно-технических и художественных изданий расширяет кругозор студентов и способствует их всестороннему развитию.

Таким образом, библиотека колледжа является ключевым элементом образовательного процесса, обеспечивая студентов и преподавателей

необходимыми ресурсами для эффективного обучения и научной деятельности.

Для расчетов, производимых студентами в процессе выполнения курсовых и дипломных проектов, библиотека предлагает воспользоваться информационно-поисковыми системами «Техэксперт» и «Консультант +», которые предоставляют образцы документов и формы отчетности; нормы, правила, стандарты, справочную информацию.

Проблему книгообеспеченности библиотека колледжа решает путём сочетания традиционных методов заказа учебной литературы и использования её в учебном процессе с применением электронных изданий. Преподавателями ГБПОУ «ЮУрГТК» разработано более 2000 электронных образовательных курсов, размещенных в СДО колледжа dom.sustec.ru [48].

Коллекции электронных документов составляют цифровую библиотеку. Одной из составляющей частей электронной библиотеки являются электронные библиотечные системы. Сотрудники библиотеки проводят обучающие занятия для студентов первых курсов и в рамках школы молодых педагогов для преподавателей, где рассказывают и показывают приёмы работы с ЭБС.

Использование библиотеками социальных сетей для взаимодействия с аудиторией стало важным инструментом в современном мире. Вот несколько ключевых преимуществ этого подхода:

1) Расширение охвата аудитории. Социальные сети предоставляют возможность выйти за пределы традиционных каналов коммуникации и привлечь внимание новой аудитории, включая молодежь, которая часто проводит время в Интернете.

2) Повышение вовлеченности читателей. Разнообразный контент, такой как анонсы мероприятий, обзоры книг, цитаты известных авторов, викторины и конкурсы, помогает заинтересовать подписчиков и повысить их активность.

3) Обратная связь и взаимодействие. Читатели могут оставлять комментарии, задавать вопросы и предлагать идеи, что позволяет библиотеке лучше понять потребности посетителей и адаптировать свои услуги.

4) Информирование о событиях и новинках. Быстрое оповещение о выставках, лекциях, встречах с авторами и новых поступлениях помогает держать аудиторию в курсе последних событий.

5) Увеличение посещаемости мероприятий. Активное продвижение мероприятий через социальные сети может привести к увеличению числа участников, особенно если используются рекламные кампании.

6) Персонализация контента. Возможность создания тематических групп и страниц позволяет библиотекам сегментировать аудиторию и предоставлять релевантную информацию каждому сегменту.

7) Укрепление имиджа библиотеки. Регулярное обновление страницы и публикация качественного контента помогают создать положительный образ библиотеки как современной структуры колледжа.

8) Снижение затрат на рекламу. Социальные сети являются бесплатным или недорогим каналом продвижения, что особенно актуально для государственных учреждений с ограниченным бюджетом.

9) Взаимодействие с партнерами. Сотрудничество с другими культурными организациями, издательствами и писателями через социальные сети может способствовать совместному проведению мероприятий и обмену опытом.

10) Поддержка удаленных пользователей.

Таким образом, использование социальных сетей позволяет библиотекам оставаться актуальными и востребованными в эпоху цифровой трансформации, привлекая новую аудиторию и поддерживая интерес у постоянных читателей.

Образовательная организация ГБПОУ «Южно-Уральский государственный технический колледж» создает условия для того, чтобы студенты могли получить необходимые профессиональные компетенции.

Таким образом, можно сделать вывод: информационная среда ГБПОУ «Южно-Уральский государственный технический колледж» включает различные элементы, которые обеспечивают доступ студентов, преподавателей и сотрудников к необходимой информации и ресурсам для обучения и работы.

Основные компоненты информационной среды ЮУрГТК:

1. Электронная информационно-образовательная среда:

– платформа дистанционного обучения (например, Moodle), которая позволяет студентам получать учебные материалы, участвовать в онлайн-занятиях, сдавать контрольные работы и тесты;

– электронный журнал успеваемости, где студенты могут отслеживать свои оценки и посещаемость;

– библиотечные ресурсы, включая электронные учебники и базы данных научных статей.

2. Корпоративная сеть:

– внутренняя локальная сеть, обеспечивающая связь между компьютерами и серверами колледжа;

– доступ к корпоративной почте и другим внутренним сервисам.

3. Официальный сайт колледжа:

– информация о колледже, его структуре, образовательных программах и мероприятиях;

– новости и анонсы событий;

– контактная информация и формы обратной связи.

4. Социальные сети и мессенджеры:

– официальные страницы колледжа в социальных сетях (ВКонтакте, Одноклассники, Telegram и др.), где публикуются новости, объявления и другая полезная информация;

– группы и чаты для общения студентов и преподавателей на платформе Сферум.

5. Технические средства обучения:

– компьютерные классы с современным оборудованием;

– лаборатории и мастерские, оснащенные необходимым инструментарием для практических занятий.

6. Библиотека:

– традиционные печатные издания;

– электронные библиотеки и каталоги.

7. Системы управления и мониторинга:

– системы управления учебным процессом (например, система "1С: Образование");

– системы мониторинга посещаемости и успеваемости студентов на платформе Сетевой город. Образование.

8. Кибербезопасность:

– защита информационных систем от несанкционированного доступа и утечек данных;

– антивирусные программы и межсетевые экраны.

Таким образом, информационная среда ЮУрГТК представляет собой комплексную систему, включающую цифровые платформы, технические средства и сервисы, направленные на обеспечение качественного образовательного процесса и поддержку взаимодействия всех участников учебного процесса.

2.2 Мероприятия по формированию основ кибербезопасности

Россия является одним из мировых лидеров по числу интернет-пользователей, и это не случайно. Россия занимает первое место в Европе и шестое – в мире по количеству пользователей Интернета. Более 70 млн человек в Российской Федерации активно используют цифровые сервисы и

ИКТ-технологии, более 20 млн человек в стране задействованы в информационной индустрии. В последние десятилетия страна сделала значительные шаги в области цифровизации, внедрив передовые информационные технологии практически во все сферы жизни: образование, здравоохранение, государственные услуги, бизнес и многие другие.

В современном обществе образование является главной составляющей жизни любого человека. Оно способствует развитию и достижению успеха в различных областях жизни не только подрастающего поколения, но и взрослых. При обучении каждый приобретает новые компетенции и ценности, поэтому важно обеспечить их эффективность.

Федеральный закон «Об образовании» гласит, что «Образование – единый целенаправленный процесс воспитания и обучения, являющийся общественно значимым благом и осуществляемый в интересах человека, семьи, общества и государства, а также совокупность приобретаемых знаний, умений, навыков, ценностных установок, опыта деятельности и компетенции определенных объема и сложности в целях интеллектуального, духовно-нравственного, творческого, физического и (или) профессионального развития человека, удовлетворения его образовательных потребностей и интересов» [13].

В последнее время перед государством и профессиональными сообществами (преподавателями, психологами, юристами, разработчиками программного обеспечения и др.) встала задача разработки системы мер, которая бы дала возможность, во-первых, эффективно обеспечить информационную безопасность студентов, и, во-вторых, использовать весь арсенал средств современной педагогики для формирования у обучающихся учебных заведений цифровых навыков.

Вопросы обеспечения кибербезопасности обучающихся являются одной из ключевых проблем подрастающего поколения в современной России. По различным данным в России каждый день в глобальную сеть

заходит более 80% всех обучающихся, при этом более 90% сталкиваются с различными проблемами в сети Интернет.

Достаточно только перечислить хотя бы малую часть из тех рисков, которым подвержен студент профессиональной образовательной организации:

1) Негативное эмоциональное состояние:

– Тревога. Это чувство беспокойства, напряжения или страха перед неопределенностью будущего. Она может проявляться как в виде общего состояния, так и в форме конкретных фобий. Длительная тревога может привести к развитию тревожных расстройств, которые требуют профессиональной помощи.

– Страх. Это реакция организма на реальную или воображаемую угрозу. Страх может быть полезным механизмом защиты, но если он становится чрезмерным и мешает нормальной жизни, это может указывать на наличие фобии или других психологических проблем.

2) Опасность киберзависимости:

– Привыкание к сетевым играм и другим сервисам Интернета может приводить к зависимости, которая называется интернет-зависимостью или киберзависимостью. Это состояние характеризуется неспособностью контролировать время, проведенное за компьютером или смартфоном, что негативно сказывается на социальной жизни, учебе или работе.

– В некоторых случаях зависимость от игр может вызывать проблемы со сном, ухудшением физического здоровья, а также социальную изоляцию.

3) Опасность проблем, связанных с сексуальным поведением.

4) Опасность поведения, связанного с риском для жизни или опасного для здоровья (употребление психотропных препаратов, суицидальное поведение).

5) Опасность кибербуллинга (травля в сети Интернет). Кибербуллинг – это форма травли, которая происходит через интернет и другие цифровые платформы. В отличие от традиционной травли, он может происходить круглосуточно, распространяться мгновенно среди большого числа людей и оставлять следы, которые сложно удалить. Кибербуллинг представляет собой серьезную угрозу для общества, требующую комплексного подхода к решению [46].

Молодые люди зачастую не осознают всех рисков, связанных с использованием Интернета. Они могут случайно стать жертвами мошенничества, фишинга, кибербуллинга, кражи личных данных или другого рода кибератак. Интернет полон опасностей, таких как вирусы, шпионские программы, спам и нежелательный контент. Подросткам нужно знать, как распознавать и избегать подобных угроз. Социальные сети играют огромную роль в жизни подростков, но они также могут стать источником опасности. Важно научить молодых людей правилам безопасного поведения в социальных сетях, чтобы избежать кибербуллинга, манипуляций и утечки личной информации. Подростки часто не задумываются о последствиях публикации личной информации в сети Интернет. Им следует объяснять, что всё, что они размещают в сети, может остаться там навсегда и повлиять на их будущее.

Создание доброжелательной психологической атмосферы в образовательном учреждении, свободной от проявлений психологического насилия, – задача всех участников образовательного процесса: администрации учебного заведения, учителей и преподавателей, родителей и, конечно же, самих обучающихся и студентов. Воспитание доброжелательного отношения к людям, уважение к личности каждого – важнейшая задача всех институтов социализации [50]. Важно воспитывать у молодежи понимание этики и ответственности в цифровой среде. Это поможет предотвратить распространение оскорбительного контента, нарушения авторских прав и других негативных действий.

В Российской Федерации действует проект «Цифровая Россия», некоторыми направлениями которого являются:

1) Поддержка российских ИТ-компаний. Поддержка отечественных компаний в сфере информационных технологий способствует развитию инноваций, созданию новых рабочих мест и укреплению конкурентоспособности страны на мировом рынке.

2) Учителя информатики. Обучение новым технологиям начинается с подготовки квалифицированных преподавателей. Поддержка учителей и преподавателей информатики включает повышение квалификации, разработку современных учебных программ и обеспечение доступа к необходимым ресурсам.

3) Доступная и безопасная цифровая среда. Создание условий для безопасного использования интернета всеми пользователями, включая защиту персональных данных, борьбу с киберпреступностью и обеспечение равного доступа к цифровым услугам независимо от географического положения или социального статуса.

4) Киберспорт. Киберспорт стремительно развивается во всем мире, и поддержка этого направления помогает привлечь молодых людей к занятиям спортом, развивает навыки стратегического мышления и командной работы, а также создает новые возможности для бизнеса и индустрии развлечений.

5) Отечественные цифровые сервисы и платформы социальной направленности. Развитие таких сервисов позволяет создавать удобные и доступные инструменты для взаимодействия граждан с государством, бизнесом и друг с другом, что улучшает качество жизни и повышает уровень доверия к государственным и частным инициативам.

6) Цифровой патриотический контент. Создание и распространение контента, направленного на воспитание патриотизма среди молодежи, имеет важное значение для формирования у подрастающего поколения чувства гордости за свою страну, ее историю и достижения[14].

Реализация этих направлений требует комплексного подхода, включающего государственное финансирование, законодательную поддержку, образовательные программы и активное участие бизнеса. Успешная реализация проекта позволит стране занять лидирующие позиции в глобальном технологическом пространстве и обеспечить устойчивое социально-экономическое развитие.

В Концепции информационной безопасности детей в Российской Федерации, утвержденной Распоряжением Правительства Российской Федерации от 28 апреля 2023 г. № 1105-р, было четко сформулировано: «В целях формирования у детей и подростков правильного безопасного алгоритма поведения в сети «Интернет» необходимо: провести анализ образовательных программ, а также факультативных учебных предметов, курсов, дисциплин, предлагаемых образовательными организациями; сформировать и интегрировать в образовательный процесс уроки информационной безопасности и цифровой грамотности детей; проводить на постоянной основе просветительские мероприятия, направленные на информирование о правилах безопасного пользования детьми сетью «Интернет», средствах защиты несовершеннолетних от доступа к информации, наносящей вред их здоровью, нравственному и духовному развитию, предназначенных для родителей (законных представителей), работников системы образования, специализированных государственных детских и юношеских библиотек и других специалистов, занятых обучением и воспитанием несовершеннолетних, организацией их досуга» [5].

Ориентация на формирование определенных личностных качеств выпускников является важным элементом современного образования в соответствии с федеральным государственным образовательным стандартом среднего общего образования. В данном случае речь идет о развитии таких характеристик, как готовность к сотрудничеству,

способность к учебно-исследовательской, проектной и информационно-познавательной деятельности [4].

Министерство просвещения является участником Федерального проекта «Цифровая образовательная среда», который направлен на создание и внедрение в образовательных организациях цифровой образовательной среды, а также обеспечение реализации цифровой трансформации системы образования. В рамках проекта ведется работа по оснащению организаций современным оборудованием и развитию цифровых сервисов и контента для образовательной деятельности [17].

Следовательно, комплекс мероприятий по формированию информационной и кибербезопасности легко встроить в образовательный процесс ПОО, причем лучше всего это делать систематически с планированием и аналитическим отчетом о результатах.

Что можно делать для повышения кибербезопасности в образовательных организациях?

1) Проведение лекций и тренингов. Регулярное информирование студентов о правилах безопасной работы в интернете, защите персональных данных и мерах предосторожности.

2) Использование специализированных программ и приложений. Установка антивирусных программ, фильтров контента и других защитных мер на компьютерах и устройствах, используемых в учебных заведениях.

3) Разработка правил поведения в сети Интернет. Создание и внедрение четких правил использования интернета и цифровых устройств в образовательных учреждениях, соблюдение которых будет обязательным для всех студентов, преподавателей и сотрудников ПОО.

4) Обратная связь и поддержка. Организация консультаций и горячих линий, куда студенты смогут обратиться за помощью в случае возникновения проблем или вопросов, связанных с безопасностью в Интернете.

5) Привлечение родителей. Родителям тоже стоит рассказывать о важности информационной и кибербезопасности, чтобы они могли поддерживать своих детей дома, оказывать помощь в соблюдении правил безопасного поведения в сети Интернет.

Однако педагоги и сами должны овладеть набором компетенций, необходимых для получения, понимания, адаптации, создания, хранения и представления информации для анализа проблем и принятия решений, и развивать эти способности в своих студентах. Существуют компетенции, применимые к любому контексту в рамках преподавания и обучения, будь то образование, общая рабочая/профессиональная среда или процесс самосовершенствования. Информационно грамотный педагог способен понимать информационные и медийные сообщения, поступающие из различных источников информации; он может оценивать и надлежащим образом использовать это понимание для решения проблем [38].

Постоянное напоминание о различных аспектах информационной и кибербезопасности поможет всем участникам учебного процесса развивать осознанное отношение к этим вопросам.

Вот несколько конкретных шагов, которые можно предпринять:

Для студентов:

– Практика безопасной работы в сети Интернет. Студенты должны знать основные правила безопасного поведения в сети, такие как создание сложных паролей, использование двухфакторной аутентификации, осторожное обращение с электронной почтой и социальными сетями.

– Изучение принципов антивирусной защиты. Необходимо объяснить, как работают антивирусы и почему они важны для защиты устройств от вредоносного ПО.

– Понимание фишинга и других видов мошенничества. Студентам следует научиться распознавать подозрительные письма и сообщения, избегать перехода по сомнительным ссылкам и делиться своими личными данными только в проверенных источниках.

Для преподавателей:

– Осведомленность о рисках. Преподаватели должны быть знакомы с основными видами киберугроз и способами их предотвращения. Это поможет им лучше организовать учебный процесс и защитить свои устройства и данные.

– Использование защищенных платформ. При проведении дистанционных занятий важно выбирать платформы, обеспечивающие высокий уровень безопасности, такие как защищенные видеоконференции и облачные хранилища с шифрованием данных.

– Разработка учебных материалов по кибербезопасности. Преподаватели могут включать в свои учебные дисциплины специальные разделы, посвященные вопросам кибербезопасности, проводить тематические занятия.

Для администрации образовательных учреждений:

– Создание политик безопасности. Администрации образовательных учреждений должны разработать четкие инструкции и политики по обеспечению информационной безопасности, которые будут обязательны для всех участников образовательного процесса.

– Проведение тренингов и семинаров. Регулярные тренинги и семинары по кибербезопасности помогут поддерживать высокий уровень осведомленности среди всего педагогического коллектива и сотрудников образовательной организации.

– Техническая поддержка. Важно обеспечить своевременное обновление программного обеспечения, установку антивирусных программ и проведение регулярных проверок на наличие уязвимостей [52].

Такие меры помогут защитить всех участников образовательного процесса от потенциальных угроз в интернете и сформировать у них ответственное отношение к использованию цифровых технологий.

В рамках формирования безопасного поведения в информационно-коммуникационной сети Интернет предлагаю для студентов

профессиональных образовательных организаций проводить олимпиады по безопасности в сети Интернет, курсы по повышению информационной грамотности, киберуроки, классные часы, квизы, викторины, деловые игры, квесты, проектные работы, круглые столы, конкурсы рисунков и электронных публикаций, встречи с экспертами и т.д. Форма может быть разная, главное, что цель мероприятий одна: формирование кибербезопасности у студентов ПОО. В комплексе данные мероприятия будут формировать у студентов основы кибербезопасности и в дальнейшем обеспечат профессиональное становление выпускника профессиональной образовательной организации, что сделает его более конкурентоспособным специалистом на рынке труда в современном информационном пространстве.

Реализация мероприятий по формированию кибербезопасности студентов колледжа происходит путем внедрения в образовательный процесс активных методов обучения на протяжении всего периода обучения на аудиторных и внеаудиторных занятиях общеобразовательной дисциплины Информатика.

Приведем примеры некоторых мероприятий.

Киберуроки по информационной безопасности познакомят с правилами безопасной работы в сети Интернет и научат ориентироваться в информационном пространстве [53]. Киберуроки способствуют ответственному использованию online-технологий, формируют информационную культуру студентов, развивают критическое мышление. Методическая разработка одного киберурока приведена в приложении №1.

Олимпиада «Безопасный интернет» на платформе uchi.ru учит разумному и безопасному поведению в сети, объясняет основные правила использования электронных средств с выходом в Интернет, развивает навыки работы с информацией, логическое мышление и память, демонстрирует реалистичные ситуации, учит принимать взвешенные решения [40].

Онлайн-викторина «Безопасное поведение в сети Интернет», подготовленная Центром правовой информации, поможет организовать проверку знания обучающихся в области информационной безопасности [41]. Викторина закрепляет правила ответственного и безопасного поведения в сети Интернет, способы защиты от противоправных посягательств в сети Интернет и мобильной связи; поможет узнать, как избежать вредной и опасной информации, как общаться в социальных сетях (сетевой этикет), не обижая своих виртуальных друзей. Методическая разработка викторины приведена в приложении №2.

Квиз по информационной безопасности познакомит с информационной безопасностью и возможными способами применения современных методов и средств защиты информационных ресурсов, персональных данных. Методическая разработка квиза приведена в приложении №3.

В настоящее время в информационно-коммуникационной сети Интернет можно найти онлайн-квизы. Квиз (или квиз-игра) действительно может стать отличным инструментом для профориентации и обучения, особенно когда речь идет о таких важных темах, как цифровая безопасность. Вот почему этот формат может быть полезен. Преимущества использования Квизов для обучения цифровой безопасности:

– Интерактивность и увлекательность. Квиз-игры привлекают внимание благодаря своему игровому формату. Участники получают удовольствие от процесса, что повышает мотивацию к обучению.

– Геймификация. Элементы соревнования, награды за правильные ответы и прогресс создают дополнительную мотивацию. Игроки стремятся улучшить свои результаты, что стимулирует повторное прохождение игры и углубленное изучение материала.

– Мгновенная обратная связь. В отличие от традиционных методов обучения, где оценка знаний происходит после завершения всего курса, в

квизе участники сразу видят результат своих ответов. Это помогает быстрее выявлять пробелы в знаниях и корректировать обучение.

– Простота восприятия. Вопросы и задания в квизах обычно кратки и понятны, что делает материал доступным. Это особенно полезно при изучении сложных тем, таких как кибербезопасность.

– Возможность повторного прохождения. Если участник ошибся, он может попробовать снова, что способствует закреплению знаний. Повторение помогает лучше усвоить материал.

– Коллективное участие. Квиз-игры могут проводиться в группах, что развивает навыки командной работы и коллективного решения задач. Это также способствует обсуждению вопросов безопасности в цифровой среде.

– Профориентация. Квиз может включать вопросы, связанные с профессиями в сфере IT и кибербезопасности, что позволит участникам узнать больше об этих направлениях и возможно заинтересоваться ими.

КиберКвиз может помочь в обучении культуре безопасности в цифровой среде:

1) Изучение основных понятий. Квиз может содержать вопросы о том, что такое фишинг, вирусы, пароли, двухфакторная аутентификация и другие важные термины. Это поможет участникам освоить базовые правила безопасного поведения в интернете.

2) Практические советы. Вопросы могут касаться конкретных ситуаций, например, как распознать подозрительное письмо или что делать, если аккаунт был взломан. Это научит игроков применять полученные знания на практике.

3) Игровые сценарии. В игре могут быть представлены ситуации, требующие принятия решений, связанных с безопасностью. Например, нужно выбрать правильный пароль или определить, какой сайт является безопасным.

4) Оценка рисков. Участникам предлагается оценить вероятность того или иного риска в цифровой среде, что учит критически мыслить и оценивать потенциальные угрозы.

5) Знакомство с современными технологиями. Квиз может включать вопросы о новых технологиях и инструментах, используемых для обеспечения безопасности, что расширяет кругозор участников.

Пример структуры КиберКвиза:

1) Разминка. Простые вопросы о базовых понятиях кибербезопасности.

2) Основная часть. Сложные вопросы, требующие анализа и применения знаний.

3) Финальный раунд. Сценарные задачи, где необходимо принять решение в сложной ситуации.

4) Итоги. Обсуждение результатов, разбор ошибок и рекомендации по дальнейшему изучению темы.

Таким образом, например, разработанный КиберКвиз Первых в рамках проекта «Азбука кибербезопасности» станет эффективным инструментом для повышения осведомленности о цифровой безопасности среди молодежи [32].

Ежегодно мы со студентами принимаем участие Всероссийском проекте «Урок Цифры». Проект АНО «Цифровая экономика» постоянно разрабатывает новые темы уроков, очень интересных для студентов, например, «Облачные технологии: в поисках снежного барса», «Искусственный интеллект: промпт-инжиниринг», «Искусственный интеллект в отраслях». В декабре 2024 года урок проводится на тему «Код города: технологии в движении» [25].

Студенты с удовольствием участвуют в мероприятиях по формированию основ кибербезопасности, получают за пройденные

мероприятия сертификаты, которые потом добавляют в свой сайт «Портфолио карьерного продвижения студентов».

Всероссийский диктант по информационным технологиям, который проводится ежегодно на сайте ит-диктант.рф это отличный инструмент для оценки уровня цифровых компетенций студентов. Включает разнообразные задания, начиная от базовых знаний по использованию компьютера и интернета, заканчивая более сложными темами, такими как блокчейн и интернет вещей. Этот подход позволяет выявить сильные и слабые стороны каждого участника диктанта, а также дает возможность получить объективную оценку своих знаний в области информационных технологий. За участие студенты получают сертификат, который показывает уровень их знаний в области информационных технологий, данный сертификат тоже добавляют в свое портфолио карьерного продвижения.

Ежегодно проводится Всероссийская акция по определению уровня цифровой грамотности «Цифровой Диктант», в котором мы принимаем участие со студентами ЮУрГТК. Организационным партнёром пятого сезона Всероссийской акции выступил Федеральный партпроект «Цифровая Россия». Партнёрство с проектом «Цифровая Россия» придаёт этой акции дополнительный вес и авторитет, а также способствует привлечению внимания к важности цифровой грамотности и компетентности в современном обществе. В 2024 году проверка знаний в области цифровой грамотности проводилась в октябре на сайте digitaldictation.ru [26].

Всероссийский урок безопасного Интернета, проводимый Лигой безопасного Интернета совместно с Министерством внутренних дел и Министерством просвещения Российской Федерации, представляет собой важное мероприятие, направленное на повышение уровня цифровой грамотности и безопасности среди учащихся школ и студентов образовательных организаций. Целью этого урока является ознакомление

молодых людей с основополагающими принципами безопасного поведения в сети, а также формирование у них навыков, необходимых для предотвращения возможных угроз и опасностей, связанных с использованием Интернета[35].

В целях формирования безопасного поведения в информационно-коммуникационной сети Интернет, предлагаю провести цикл учебных занятий «Удивительный и опасный мир Интернета», на которых актуализируются знания студентов о различных Интернет-опасностях и предупреждается Интернет-зависимость, развиваются навыки безопасного поведения в сети Интернет, формируются и развиваются навыки поведения в опасных ситуациях, связанных с Интернет-мошенничеством, Интернет-преступлениями. Методическая разработка цикла учебных занятий часов приведена в приложении №4.

На уроках информатики возможен просмотр и обсуждение фильмов социального проекта «Кибербезопасность для детей и взрослых», подготовленных Государственной образовательной платформой «Российская электронная школа» [30]. Главная страница проекта представлена на рисунке 2.

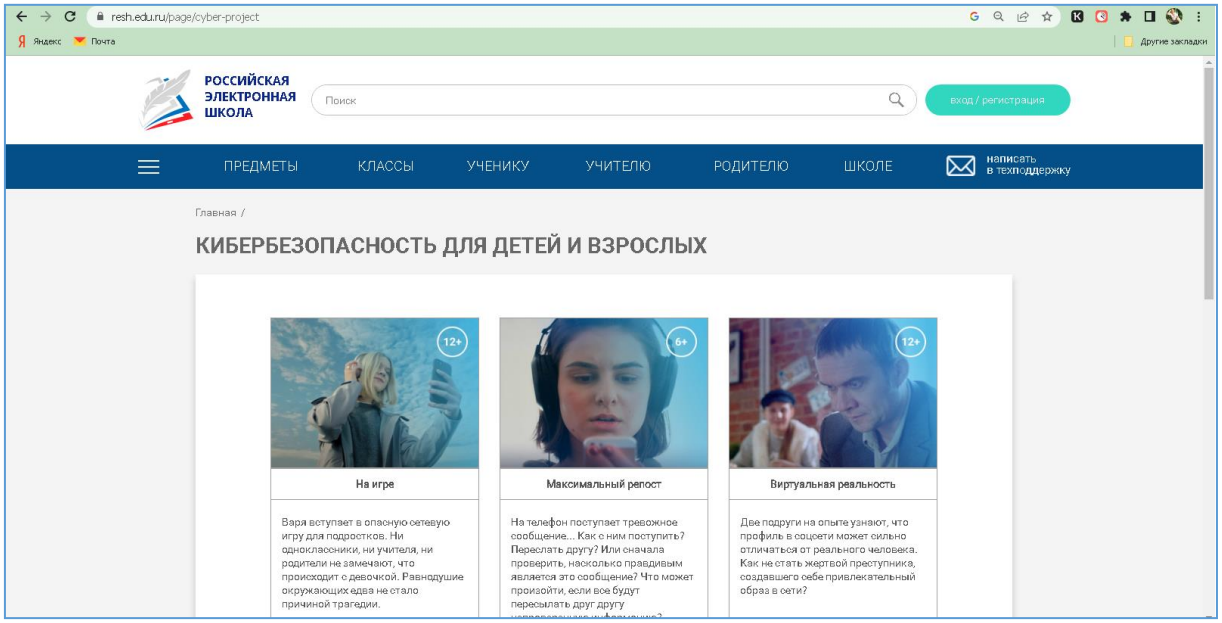

Рисунок 2 – Главная страница проекта Кибербезопасность для детей и взрослых

Еще один новый просветительский проект 2024 года от АНО «Цифровая экономика» Цифровой ликбез помогает повысить цифровую грамотность и узнать больше о кибербезопасности в сети. На сайте проекта урокцифры.рф размещены видеоролики для детей и взрослых от ведущих цифровых компаний-лидеров: VK, Благотворительный фонд Сбербанка «Вклад в будущее», СКБ Контур, «Лаборатория Касперского», Авито. При изучении темы «Информационная безопасность» знакомлю студентов с данным проектом [25].

Деловая игра, например, «Суд над Интернетом» поможет сформировать знания о пользе или вреде Интернета; ознакомить с преимуществами и опасностями Интернета; развивать навык дискуссии.

С родителями необходимо вести постоянную разъяснительную работу, т.к. без понимания родителями данной проблемы невозможно ее устранить силами только образовательного учреждения. Формы работы с родителями могут быть разнообразны: выступления на родительских собраниях, индивидуальные беседы, информация на сайте учебного заведения, встречи со специалистами, семинарские занятия [47].

Встречи с психологами и со специалистами службы безопасности были бы огромной помощью семьям студентов. А если привлекать к процессу обучения еще и специалистов в области защиты информации, представителей правоохранительных органов, программистов, тогда данное направление будет еще более эффективным.

Учебные программы по обучению и повышению осведомленности об информационной безопасности являются важнейшим элементом стратегии повышения кибербезопасности среди студентов и взрослого населения. Комбинирование различных методов обучения, таких как учебные занятия и олимпиады, диктанты и викторины, игры и симуляции, позволяет эффективно передавать знания и формировать навыки, необходимые для безопасного поведения в цифровой среде. Поэтому к вопросам обучения кибербезопасности надо подходить комплексно.

Участие студентов в конференции по информационной безопасности «гИБЧе» в Челябинске, организованной Минцифры Челябинской области, играет важную роль в формировании интереса к теме кибербезопасности и защите информации. Это яркое событие предоставило студентам уникальную возможность познакомиться с новейшими разработками и решениями в области кибербезопасности, а также пообщаться с профессионалами и экспертами. Посещение выставки «Кибербезопасность реальности» в рамках вышеназванной конференции позволило не только познакомиться с новыми продуктами и услугами, предлагаемыми российскими компаниями для защиты информации, но и понять, какие современные технологии применяются для борьбы с киберугрозами, оценить масштабы и разнообразие решений, предлагаемых на рынке кибербезопасности, узнать о новых вызовах и проблемах, стоящих перед отраслью, и о том, как компании решают эти задачи.

Таким образом, участие студентов в научно-практических конференциях и выставках по информационной безопасности является важным шагом на пути к становлению высококвалифицированных специалистов, готовых противостоять современным киберугрозам, обеспечивать безопасность в цифровом пространстве и формирующим основы кибербезопасности.

Сегодня многие коммерческие организации участвуют в просветительских проектах в сфере кибербезопасности и наработанные ими материалы необходимо использовать в учебном процессе.

1. АО «Лаборатория Касперского» разработало бесплатный ресурс материалов Kaspersky Resource Center со статьями о безопасности в Интернете, новости о последних угрозах и советы о том, как себя безопасно вести в сети [54]. Главная страница ресурса представлена на рисунке 3.

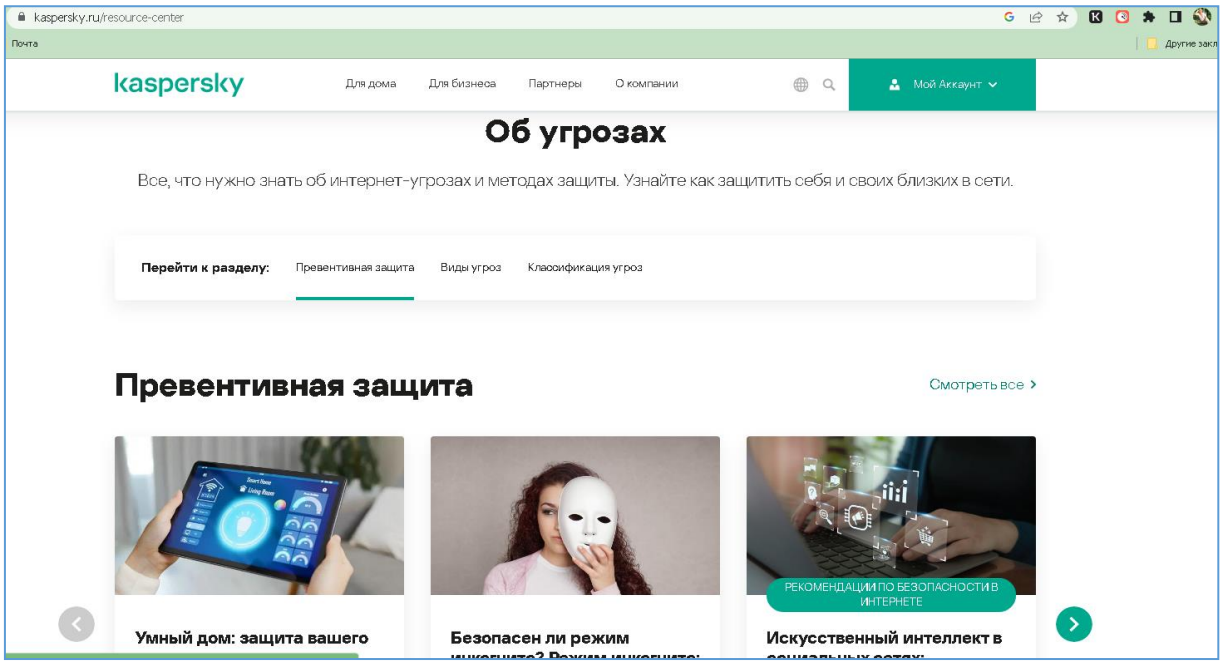

Рисунок 3 – Главная страница ресурса Kaspersky Resource Center

2. ПАО «Сбербанк» разработал страницу http://www.sberbank.ru/ru/person/ cybersecurity, посвященную безопасности в сети Интернет, кроме того разработаны памятки, которые помогут разобраться в вопросах кибербезопасности [39]. Главная страница ресурса представлена на рисунке 4.

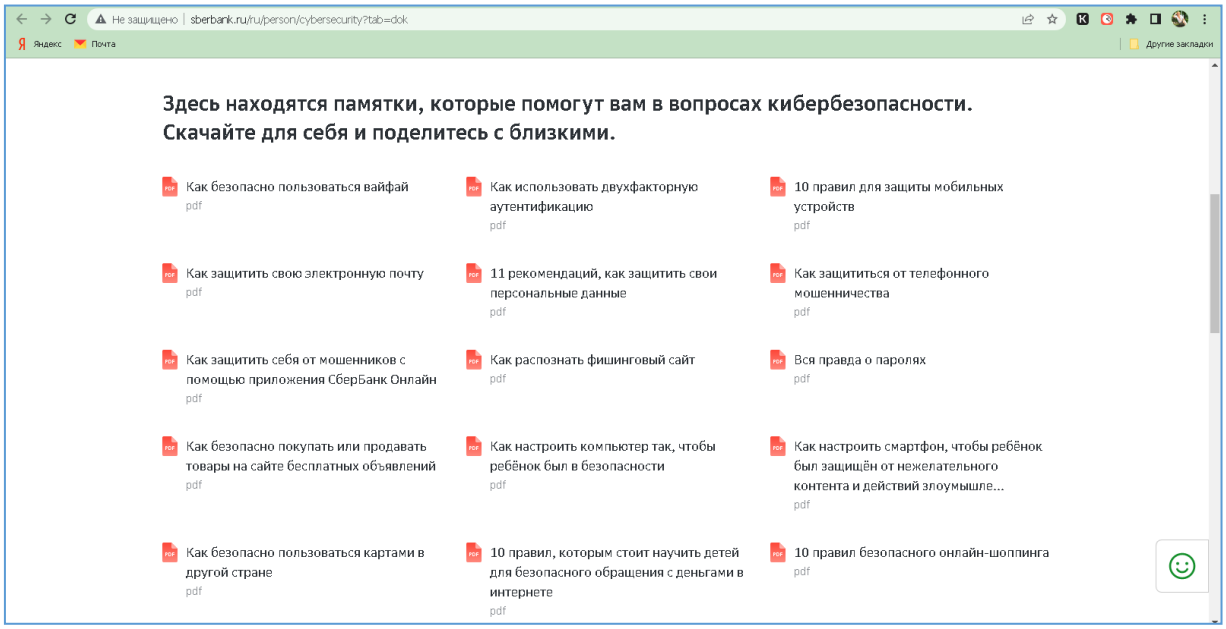

Рисунок 4 – Главная страница ресурса по безопасности в сети Интернет ПАО Сбербанк (памятки)

Сбербанк активно работает над усилением своей кибербезопасности, внедряя новые методы защиты и привлекая высококвалифицированных

специалистов. Банк регулярно организует и участвует в конференциях, форумах и конгрессах, посвященных вопросам кибербезопасности, что помогает обмениваться опытом и знаниями с другими участниками рынка. Кроме того, Сбербанк сотрудничает с международными организациями для решения общих проблем в этой сфере. [23].

3. ПАО «Ростелеком» разработал платформу для тестирования сотрудников и обучения навыкам практической кибербезопасности. Сервис «Управление навыками ИБ» представляет собой комплексное решение для повышения уровня кибербезопасности в компании путем обучения и проверки знаний сотрудников. Программа обучения включает в себя теоретические и практические модули, направленные на формирование базовых знаний и навыков в области информационной безопасности. После завершения курса обучения сотрудники проходят финальное тестирование, которое оценивает их уровень усвоения материала и готовность применять полученные знания на практике. Данную систему можно использовать для обучения преподавателей и сотрудников ПОО основам кибербезопасности [36].

Главная страница ресурса представлена на рисунке 5.

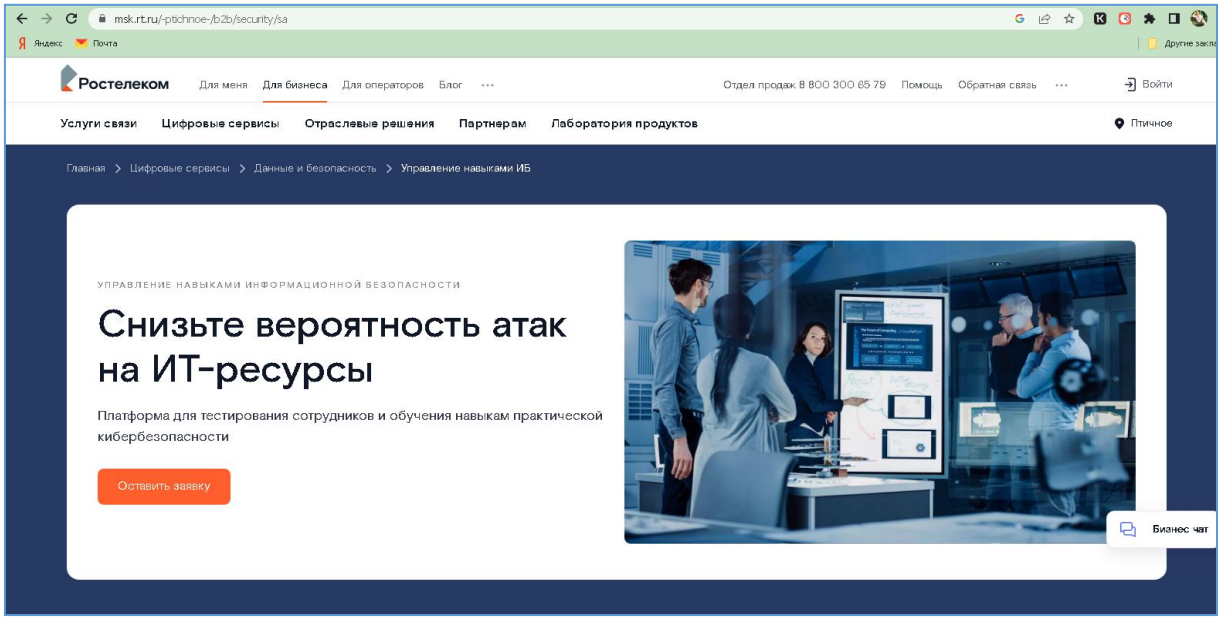

Рисунок 5– Главная страница сервиса «Управление навыками ИБ» ПАО «Ростелеком»

4. ПАО «Ростелеком» подготовил специальный онлайн-курс для родителей «Как защитить ребенка от рисков в интернете?» Взрослые узнают, как детей вовлекают в преступные группировки и какую роль в этом играет интернет, как алгоритмы, инфлюенсеры и крупные компании воздействуют на выбор ребенка и его убеждения, чем опасен кибербуллинг и как противостоять травле и домогательствам в Сети, что такое шерентинг и как защитить личные данные ребенка в интернете, чем опасны тренды и челленджи в соцсетях, а также к чему приводит интернет-зависимость. В работе приняла участие большая команда экспертов, аналитиков, профессоров, социологов, специалистов по кибербезопасности, детских психологов. Все угрозы эксперты разделили на шесть кластеров: криминализация, маркетинговое давление, психологическое насилие, цифровая эксплуатация, информационное давление и зависимость от интернет-среды. Весь курс состоит из десяти уроков. Каждому кластеру посвящено два видеоурока: в первом взрослые погрузятся в особенности и специфику каждого риска, услышат советы психолога, во втором – познакомятся с оценкой экспертов, мерами защиты и степенью их эффективности, реальными примерами столкновения детей с киберугрозами, а также узнают о рисках будущего. Главная страница ресурса представлена на рисунке 6.

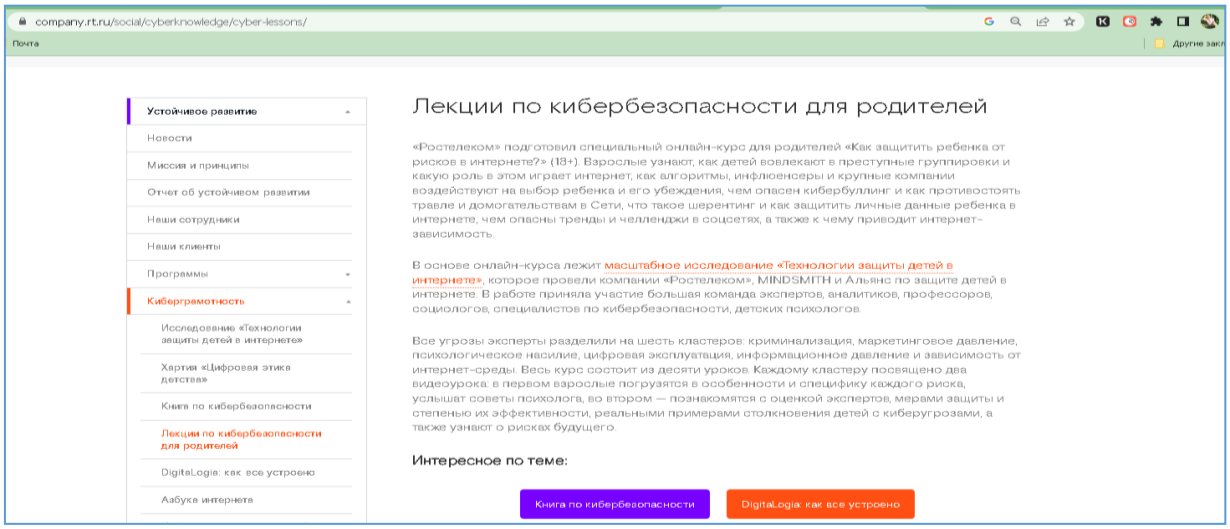

Рисунок 6– Главная страница лекций по кибербезопасности для родителей ПАО «Ростелеком»

5. Банк ВТБ предлагает в игровой форме изучить простые меры безопасности, которые защитят участников образовательного процесса от мошенников [27]. Главная страница ресурса представлена на рисунке 7.

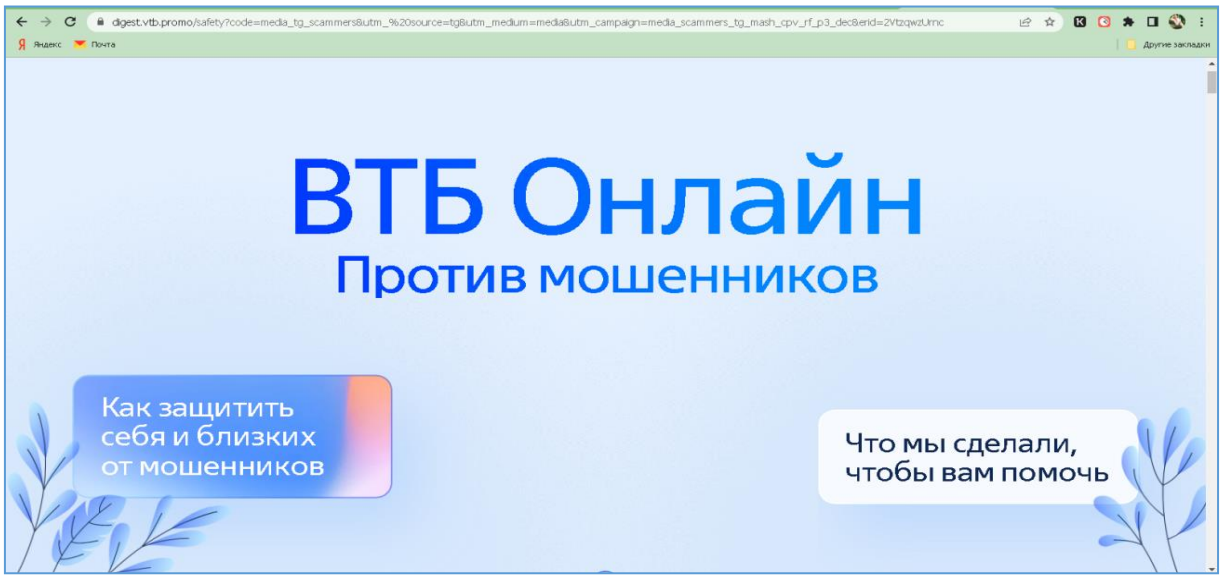

Рисунок 7– Главная страница ресурса «ВТБ онлайн против мошенников»

Основная стратегия повышения кибербезопасности заключается в сотрудничестве компаний и обмене информацией друг с другом для повышения безопасности каждого.

Реализация эффективной стратегии защиты данных поможет не только сохранить приватность и безопасность отдельных лиц и организаций, но и укрепить доверие к цифровым сервисам и платформам, способствуя дальнейшему развитию цифровой экономики.

На уроках информатики можно создавать буклеты и плакаты по информационной безопасности, писать эссе, рисовать на вышеуказанную тему, возможностей много, главное желание преподавателя развиваться самому и развивать обучающихся.

С целью формирования основ кибербезопасности у студентов ЮУрГТК был разработан учебный курс на сайте дистанционного обучения колледжа. Ссылка на ресурс https://dom.sustec.ru/course/view.php?id=260. Главная страница ресурса представлена на рисунке 8.

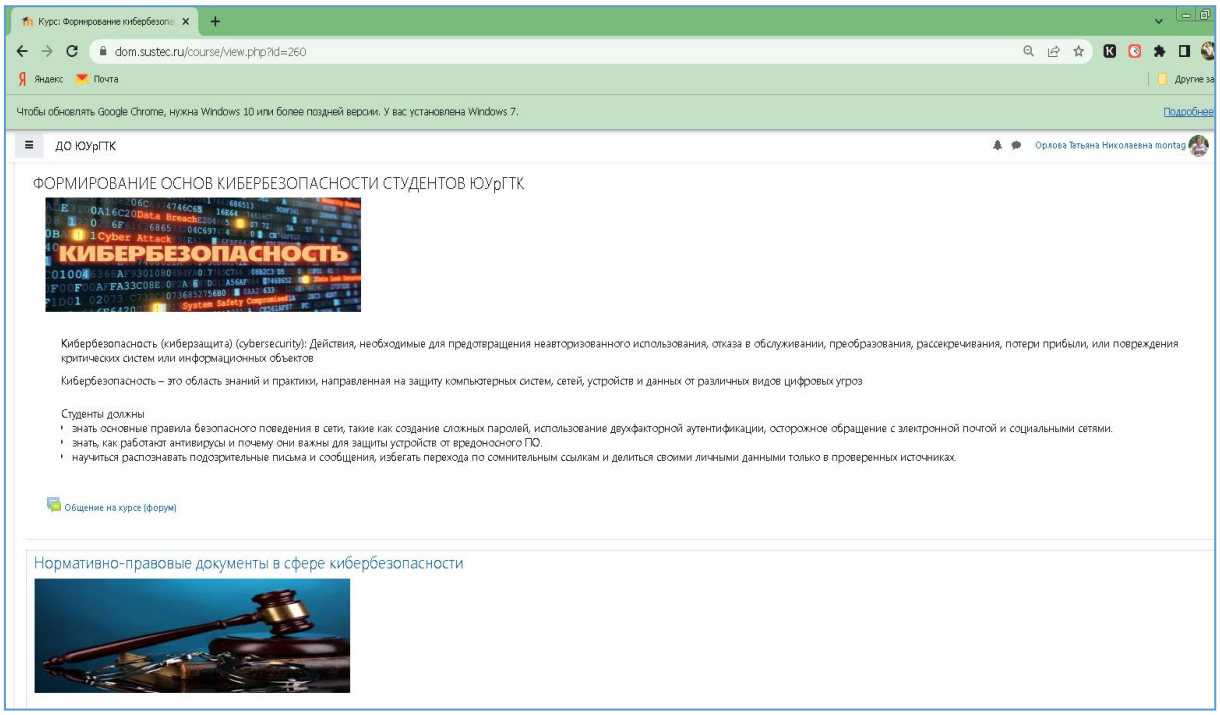

Рисунок 8– Главная страница ресурса «Формирование основ кибербезопасности студентов ЮУрГТК»

Структура курса представлена на рисунках 9 и 10:

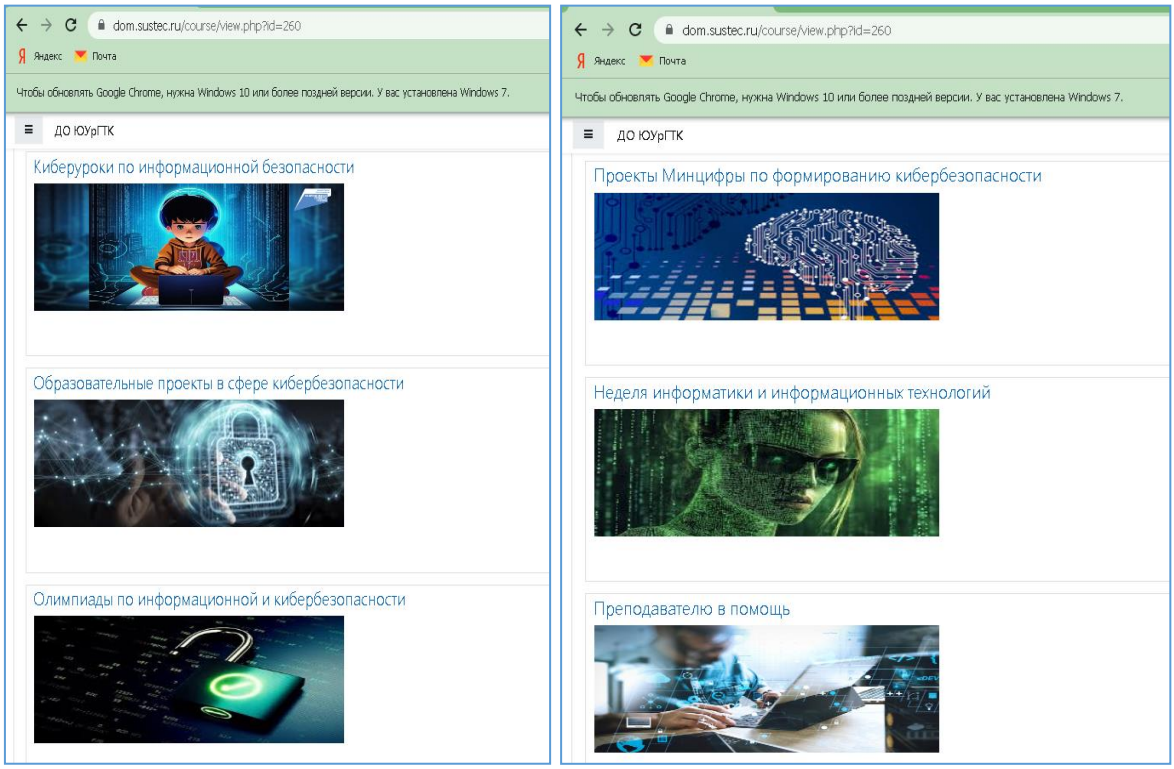

Рисунок 9– Структура ресурса «Формирование основ кибербезопасности студентов ЮУрГТК»

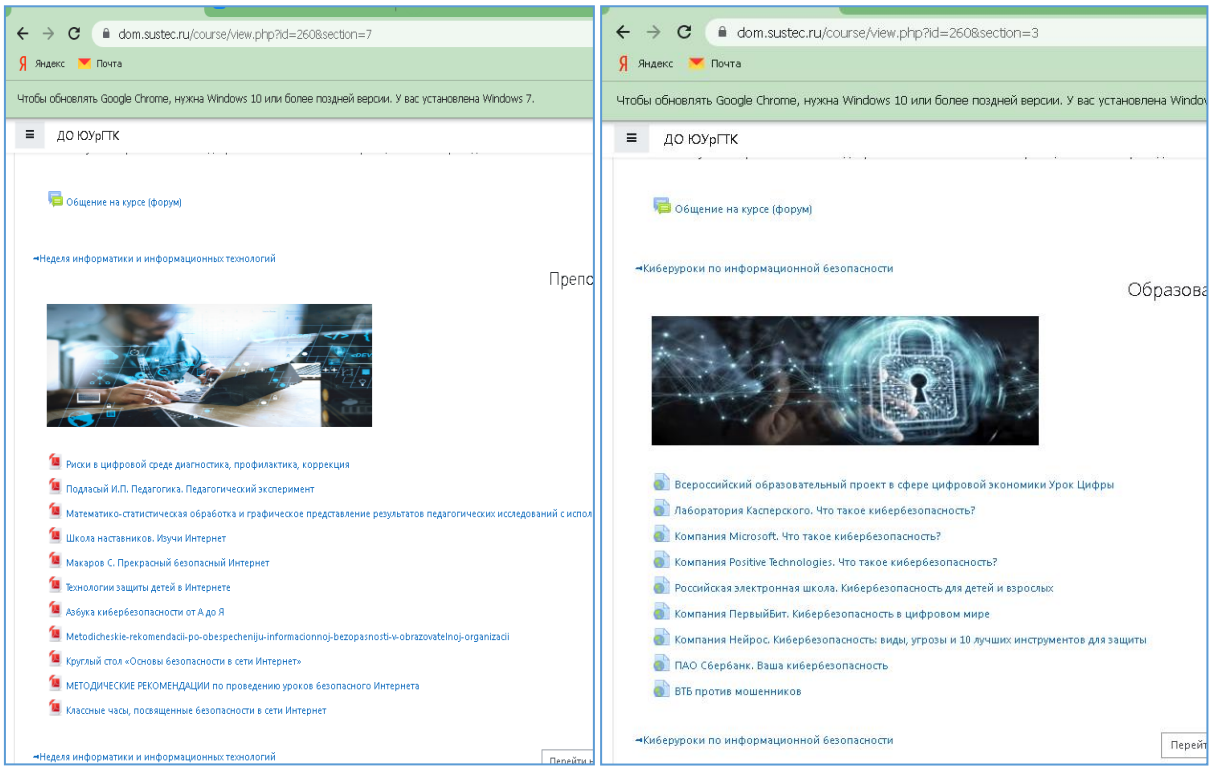

Рисунок 10–Содержание ресурса «Формирование основ кибербезопасности студентов ЮУрГТК»

Таким образом, реализация комплекса мероприятий обучающихся колледжа путем внедрения в образовательный процесс активных методов обучения на протяжении всего периода обучения студентов профессиональной образовательной организации будет способствовать формированию основ кибербезопасности.

2.3 Экспериментальная проверка мероприятий и анализ полученных результатов

Неотъемлемой частью научного исследования, в том числе и педагогического, является экспериментальная работа. Слово «эксперимент» – латинского происхождения и в переводе означает «опыт», «испытание».

Под педагогическим экспериментом в современной педагогике понимается метод исследования, который используется с целью выяснения эффективности применения отдельных методов и средств обучения и воспитания.

Задачей эксперимента является выяснение сравнительной эффективности применяемых в педагогической деятельности технологий, методов, приемов, нового содержания и т.д.[22].

По мнению Н.О. Яковлевой, «педагогический эксперимент – это комплекс методов исследования, предназначенный для объективной и доказательной проверки достоверности выдвинутой гипотезы» [57].

Известный российский ученый-педагог И.П. Подласый рассматривает педагогический эксперимент как научно организованный опыт, который направлен на преобразование педагогического процесса в строго контролируемых условиях. По его мнению, педагогический эксперимент – это метод исследования, который применяется для проверки гипотез и новых педагогических подходов в образовательных процессах. Его цель – установить причинно-следственные связи между различными факторами, влияющими на обучение и воспитание, и результатами образовательного процесса [44].

Таким образом, педагогический эксперимент – это систематизированный исследовательский процесс, целью которого является проверка гипотез и получение достоверных выводов относительно эффективности педагогических методов, приемов и технологий.

Эксперимент состоит из трех основных этапов: констатирующего, формирующего и обобщающего. Рассмотрим каждый этап подробнее.

Этапы педагогического эксперимента:

1) Констатирующий этап. На этом этапе осуществляется сбор исходных данных о состоянии исследуемого объекта (например, группе обучающихся). Проводятся предварительные замеры, анкетирования, наблюдения и другие диагностические процедуры, чтобы зафиксировать начальное состояние испытуемых. Цель этапа — установить исходный уровень знаний, умений и навыков участников эксперимента.

2) Формирующий этап. Это основной этап эксперимента, на котором реализуется педагогическое воздействие. В зависимости от поставленной цели, могут применяться разные методы обучения, образовательные технологии, дидактические средства и т.д. В ходе этого этапа фиксируются изменения, происходящие в процессе обучения, и собираются данные для последующего анализа.

3) Обобщающий (итоговый) этап. На заключительном этапе подводятся итоги эксперимента. Анализируются собранные данные, сравниваются результаты до и после эксперимента, делается вывод о достижении поставленных целей. Кроме того, формулируются выводы и рекомендации для дальнейшего использования полученных результатов в образовательной практике.

Результаты педагогического эксперимента чаще всего оцениваются по качественным критериям и показателям. В качестве критериев могут выступать:

– уровень усвоения учебного материала;

– степень сформированности навыков и умений;

– мотивация обучающихся;

– качество выполнения учебных заданий;

– психоэмоциональное состояние участников эксперимента.

Уровень развития участников эксперимента можно классифицировать следующим образом:

– низкий уровень – недостаточное владение материалом, студент имеет лишь некоторые знания по культуре информационной безопасности;

– средний уровень – удовлетворительный результат, соответствие стандартным требованиям; владение знаниями, умениями и навыками по культуре информационной безопасности;

– высокий уровень – высокие показатели, глубокое понимание и применение знаний; осознание необходимости знаний по информационной безопасности и совершенствование в данном направлении [28].

Методика проведения эксперимента. Эксперименты могут проводиться с участием экспериментальной и контрольной групп. Экспериментальная группа подвергается воздействию новых методов или технологий, тогда как контрольная группа продолжает учиться по традиционной программе. Это позволяет сравнить эффективность нововведений с существующими методами.

После проведения измерений и сбора данных выполняется математическая обработка результатов. Используются статистические методы для анализа и сравнения показателей обеих групп. Это позволяет объективно оценить влияние экспериментального воздействия.

Основная цель педагогического эксперимента заключается в том, чтобы оценить эффективность педагогического воздействия, таким образом подтвердить или опровергнуть выдвигаемую гипотезу исследования и получить практически значимые результаты исследования.

Целью проводимого мною педагогического эксперимента являлось подтверждение выдвинутой гипотезы: формирование основ кибербезопасности будет более эффективным, если выявить и реализовать комплекс мероприятий по формированию основ кибербезопасности у студентов профессиональной образовательной организации.

В процессе экспериментальной работы, для реализации цели исследования, решались следующие задачи:

1) Изучить состояние проблемы формирования готовности студентов колледжа к безопасной работе в сети Интернет.

2) Сформировать комплекс мероприятий по формирования кибербезопасности студентов ПОО и подтвердить с помощью статистического анализа эффективность педагогического эксперимента.

3) Оценить и интерпретировать полученные результаты.

Для решения задач экспериментальной работы были применены следующие методы: компьютерное анкетирование, наблюдение, собеседование, анализ рабочей программы общеобразовательной учебной

дисциплины Информатика, статистические методы для обработки данных, полученных в ходе педагогического эксперимента.

Комплексное использование данных практических методов позволяет более качественно оценить уровни готовности обучающихся на всех этапах педагогического эксперимента [29].

Экспериментальная апробация процесса формирования кибербезопасности у студентов профессиональной образовательной организации осуществлялась на базе ГБПОУ «Южно-Уральский государственный технический колледж» со студентами первого курса в течение 2023-2024 учебного года.

В исследовании приняли участие 38 обучающихся первых курсов отделения Экономики и инфраструктуры Южно-Уральского государственного технического колледжа. Было проведено диагностическое изучение, с целью выявления исходного уровня компонентов, составляющих знание информационной и кибербезопасности.

Педагогический эксперимент проводился в три этапа (констатирующий, формирующий, итоговый), на каждом из них решались определенные задачи.

Для педагогического эксперимента были выбраны две группы отделения Экономики и инфраструктуры: группа СП-117/б была контрольной, группа ЗУ-176/б являлась экспериментальной. Группы студентов, принявшие участие в эксперименте, находились в одинаковых условиях по материально-техническому и методическому обеспечению (материальной базы, образовательной среды).

Для диагностики уровня сформированности безопасного поведения в Интернете, был разработан анкетный опрос, который представлен в Приложении 5.

Всего было опрошено: 34 студента в группах СП-117/б и ЗУ-176/б.

Результаты анкетирования контрольной группы представлены в таблице, в которой указано количество правильных ответов. Каждый из студентов обозначен порядковым номером С1, С2, С3…:

Таблица 1. Сравнительные результаты входного опроса

Входной	С1	С2	С3	С4	С5	С6	С7	С8	С9	С 10	С 11	С 12	С 13	С 14	С 15	С 16	С 17	С 18	С 19
К	4	5	6	7	7	7	7	8	8	8	8	8	8	9	9				
Э	4	4	4	5	5	5	5	6	6	6	6	6	6	7	7	7	7	7	9

На рисунке 11 представлены результаты распределения данных по безопасной работе в сети Интернет контрольной группы на констатирующем этапе. Средний результат в контрольной группе 7,27.

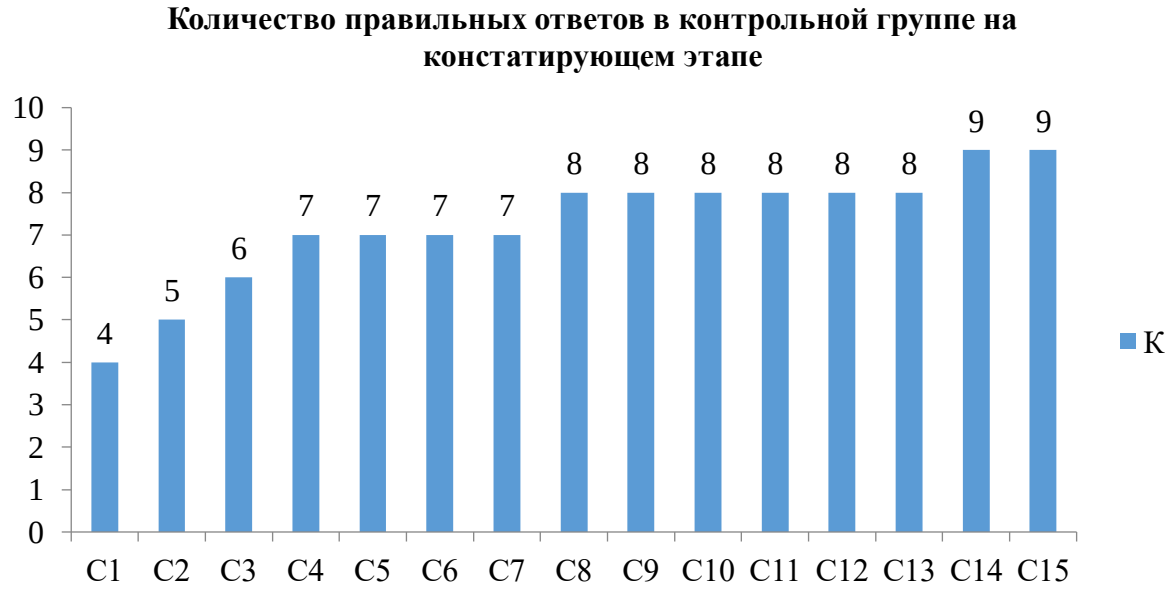

Рисунок 11 - Количество правильных ответов в контрольной группе на констатирующем этапе

На рисунке 12 представлены результаты распределения данных по безопасной работе в сети Интернет экспериментальной группы на констатирующем этапе. Средний результат в экспериментальной группе 5,89.

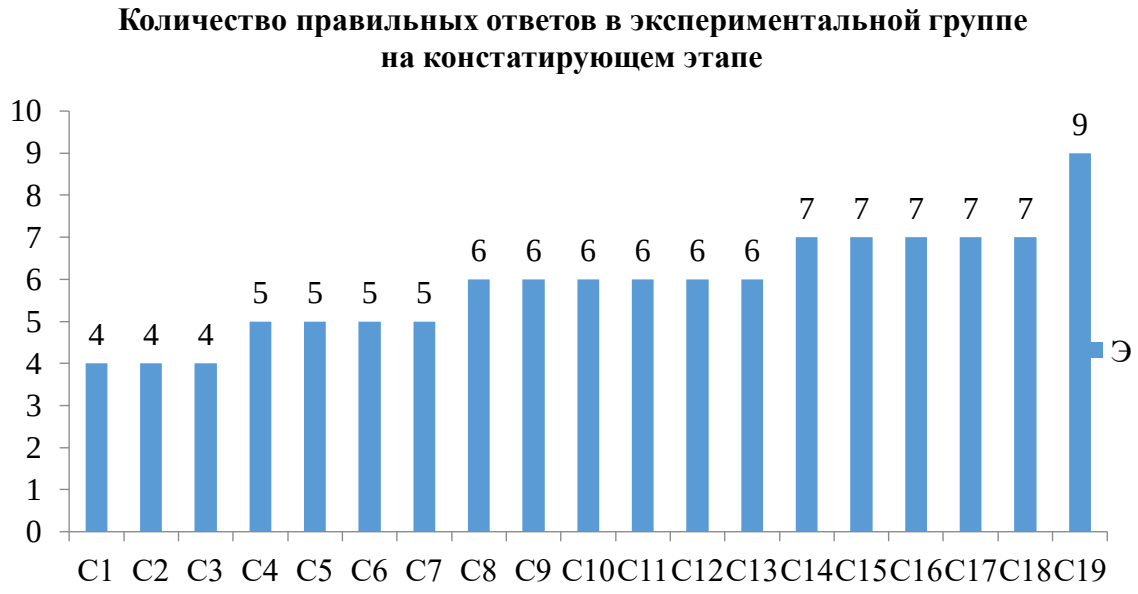

Рисунок 12 - Количество правильных ответов в экспериментальной группе на констатирующем этапе

Анализируя результаты, можно отметить, что в наших группах на итоговом этапе эксперимента преобладают студенты со средним и низким уровнем кибербезопасности.

Таблица 2. Сравнительные результаты входного опроса групп, %

Входной	С1	С2	С3	С4	С5	С6	С7	С8	С9	С 10	С 11	С 12	С 13	С 14	С 15	С 16	С 17	С 18	С 19	Среднее
К	44 %	56 %	67 %	78 %	78 %	78 %	78 %	89 %	89 %	89 %	89 %	89 %	89 %	100 %	100 %					81 %
Э	44 %	44 %	44 %	56 %	56 %	56 %	56 %	67 %	67 %	67 %	67 %	67 %	67 %	78 %	78 %	78 %	78 %	78 %	100%	61 %

Таблица 3. Оценка уровня кибербезопасности студентов на констатирующем этапе

Уровень групп	Высокий уровень, (91-100%)	Средний уровень (71-90%)	Низкий уровень (50-70%)	Очень низкий (< 50%)
К	2	10	2	1
Э	1	5	10	3

При анализе результатов, полученных при проведении данных исследований, мы можем констатировать факт того, что высоким уровнем знаний в области кибербезопасности из обеих обследованных групп обладают 1% обучающихся (3 студента); самый больший процент студентов обладает средним уровнем знаний 44% (15 студентов), низким

уровнем обладают 35% (12 студентов) и очень низким уровнем кибербезопасности обладает 1% (4 студента).

Оценка уровня кибербезопасности студентов на констатирующем этапе представлена на рисунке 13.

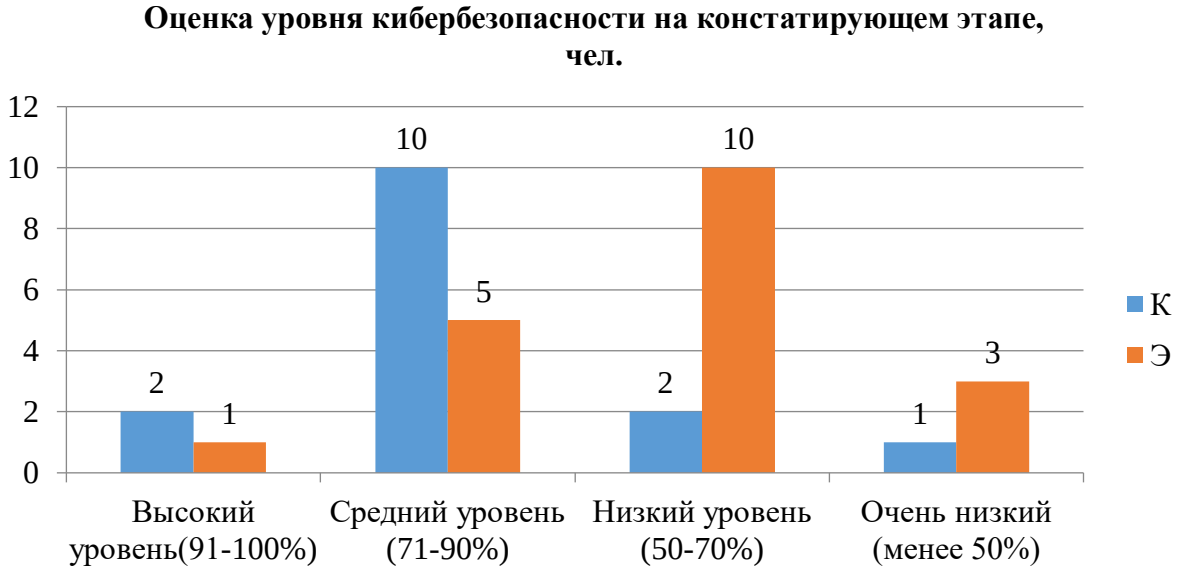

Рисунок 13 – Сравнительная характеристика уровня знаний экспериментальной и контрольной групп на констатирующем этапе

По результатам тестирования можно сделать вывод о необходимости проведения формирующей работы, которая была направлена на укрепление знаний студентов в области кибербезопасности.

На основании проведенного анализа, был составлена программа мероприятий, в которую были включены такие темы, как: информационная безопасность; кибербезопасность; Интернет и его роль в жизни современного человека; этические нормы в Интернете; средства обеспечения кибербезопасности; опасности в сети Интернет; преступления в сфере информационных технологий и способы защиты от киберпреступников.

В течение 2023-2024 учебного года с экспериментальной группой ЗУ-176/б проводились мероприятия, направленные на формирование кибербезопасности: киберуроки, викторины, квизы, просмотр фильмов, олимпиады, диктанты, цикл учебных занятий.

В конце 2023-2024 учебного года студентам были предложены те же тесты. В таблице 4 представлены сравнительные результаты повторного опроса в количестве правильных ответов на вопросы анкеты.

Таблица 4. Сравнительные результаты повторного опроса, кол-во правильных ответов

Итоговый	С1	С2	С3	С4	С5	С6	С7	С8	С9	С 10	С 11	С 12	С 13	С 14	С 15	С 16	С 17	С 18	С 19
К	9	9	9	9	9	9	8	8	7	6	7	6	7	8	8	7	7	7	7
Э	9	7	7	8	7	9	9	9	9	9	9	9	9	9	6	5	6	5	5

Результаты повторного анкетирования в контрольной и экспериментальной группах представлены на рисунках 14 и 15:

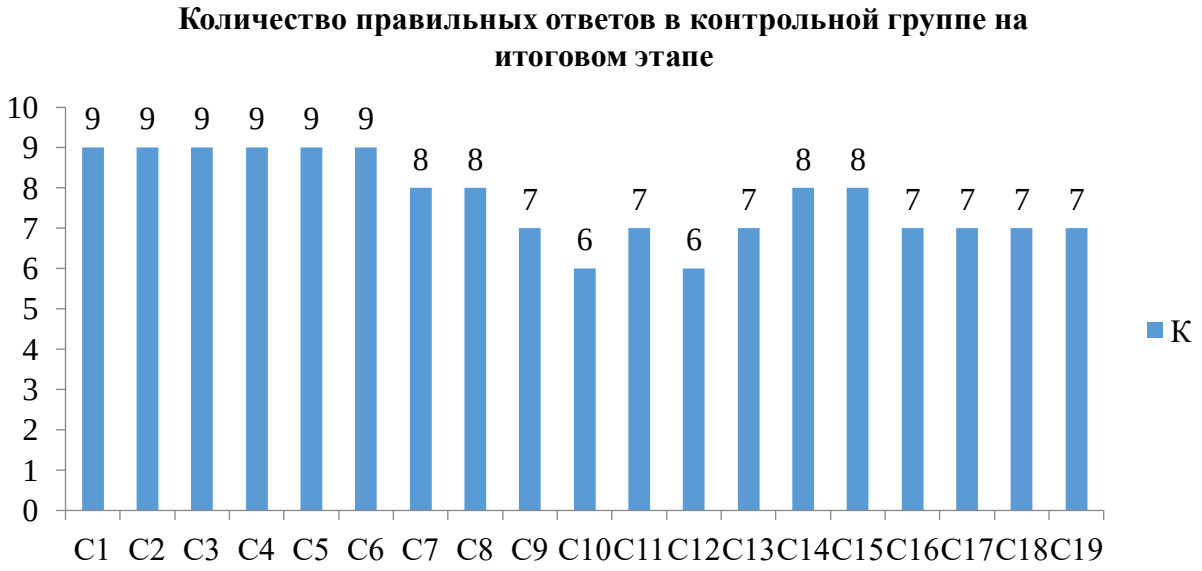

Рисунок 14–Результаты теста «Оценка уровня кибербезопасности студентов» в контрольной группе на контрольном этапе

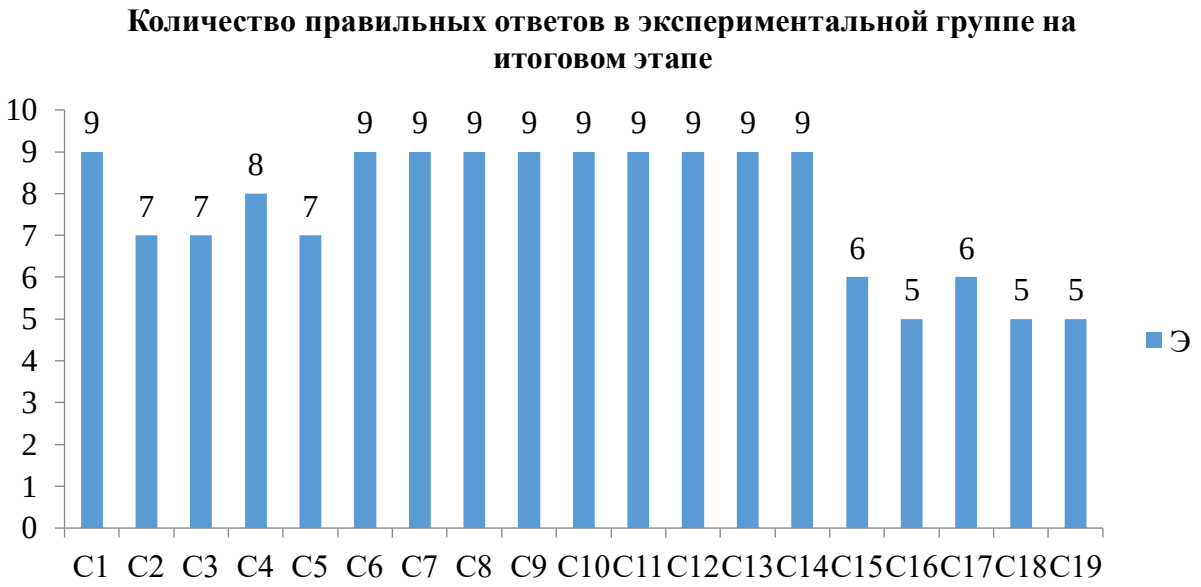

Рисунок 15 – Результаты теста «Оценка уровня кибербезопасности студентов» в экспериментальной группе на контрольном этапе

Таблица 5. Сравнительные результаты повторного опроса, %

Итоговый	С1	С2	С3	С4	С5	С6	С7	С8	С9	С 10	С 11	С 12	С 13	С 14	С 15	С 16	С 17	С 18	С 19
К	100 %	100 %	100 %	100 %	100 %	100 %	89 %	89 %	78 %	67 %	78 %	67 %	78 %	89 %	89 %	78 %	78 %	78 %	78 %
Э	100 %	78 %	78 %	89 %	78 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %	67 %	56 %	67 %	56 %	56 %

Таблица 6. Оценка уровня кибербезопасности студентов на контрольном этапе, чел.

Уровень групп	Высокий уровень, (91-100%)	Средний уровень (71-90%)	Низкий уровень (50-70%)	Очень низкий (< 50%)
К	6	11	2	0
Э	10	4	5	0

Уровень кибербезопасности студентов контрольной и экспериментальной групп на итоговом этапе представлен на рисунке 16.

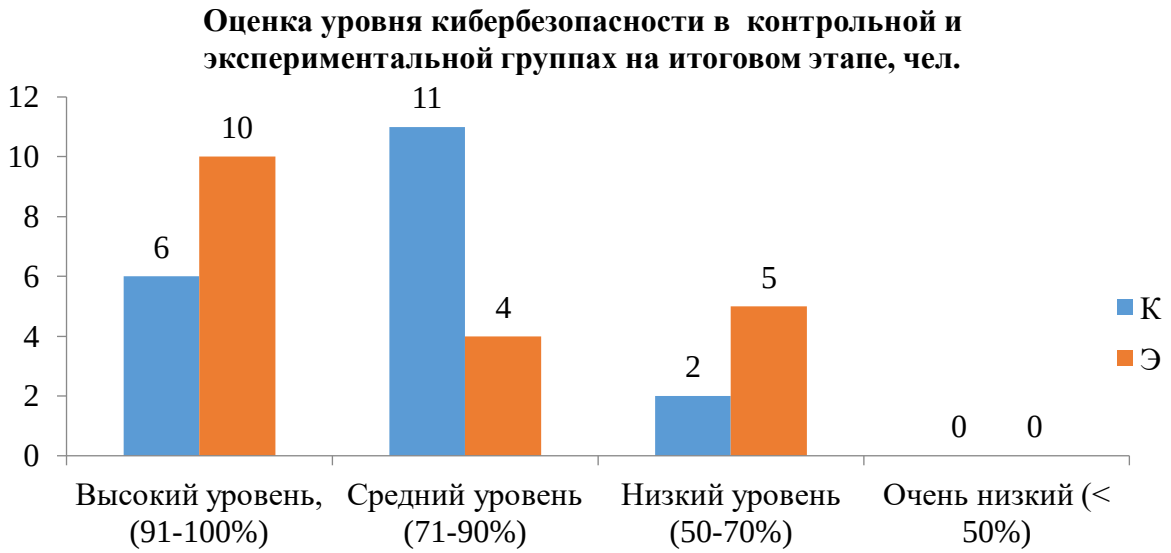

Рисунок 16 – Сравнительная характеристика уровня знаний экспериментальной и контрольной групп на контрольном этапе

Диаграммы демонстрируют, что наиболее значительные положительные изменения произошли в экспериментальной группе ЗУ-176/б, где обеспечивался весь комплекс выявленных педагогических условий, в то время как в контрольной группе изменения носят менее выраженный характер.

Докажем результативность проведенных мероприятий с помощью математической статистики, а именно t-критерия Стьюдента.

Т-критерий Стьюдента (или просто t-тест) широко используется в статистике для проверки гипотез о равенстве средних значений в двух выборках. Этот критерий позволяет сравнивать средние значения двух независимых выборок и определять, есть ли статистически значимые различия между ними. Применив t-критерий Стьюдента, мы сможем рассчитать t-статистику и определить, есть ли статистически значимая разница между группами [37].

Используя онлайн ресурс https://www.psychol-ok.ru/statistics/student, был выполнен автоматический расчет t-критерия Стьюдента:

Таблица 7. Результаты обработки уровня кибербезопасности с помощью критерия t-критерия Стьюдента

№	Выборка 1 (В.1)	Выборка 2 (В.2)	Отклонения (В.1 - В.2)	Квадраты отклонений $(В.1 - В.2)^2$
1	4	5	-1	1
2	4	5	-1	1
3	4	5	-1	1
4	5	6	-1	1
5	5	6	-1	1
6	5	7	-2	4
7	5	7	-2	4
8	6	7	-1	1
9	6	8	-2	4
10	6	9	-3	9
11	6	9	-3	9
12	6	9	-3	9
13	6	9	-3	9
14	7	9	-2	4
15	7	9	-2	4
16	7	9	-2	4
17	7	9	-2	4
18	7	9	-2	4
19	9	9	0	0
Суммы:	112	146	-34	74

Результат: $t_{Эмп} = 9.4$

Таблица 8. Критические значения

$t_{Кр}$	
p≤0.05	p≤0.01
2.1	**2.88**

Ось значимости представлена на рисунке 17:

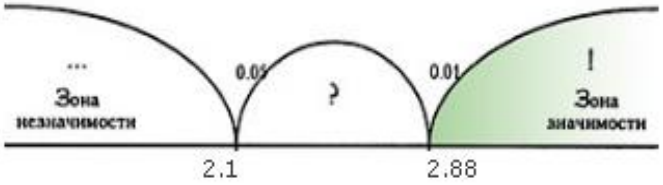

Рисунок 17 – Ось значимости результатов статистической обработки результатов методом t-критерия Стьюдента

Полученное эмпирическое значение t (9.4) находится в зоне значимости, следовательно, наша гипотеза, а именно формирование основ кибербезопасности будет более эффективным, если выявить и реализовать комплекс мероприятий по формированию основ кибербезопасности у студентов профессиональной образовательной организации, подтверждается методом математической статистики, а именно t-критерием Стьюдента [43].

Можем утверждать, что комплекс мероприятий оказал положительное влияние на студентов. Результаты педагогического эксперимента являются подтверждением того, что разработанный комплекс мероприятий действительно развивает основы кибербезопасности у студентов профессиональной образовательной организации на учебных занятиях общеобразовательной учебной дисциплины Информатика.

Полученные результаты дают основания для вывода о целесообразности внесения в педагогический процесс комплекса мероприятий, направленного на формирование кибербезопасности.

В результате педагогического эксперимента удалось прийти к выводу, что предложенный комплекс мероприятий результативен.

Выводы по главе 2

В исследовательской части работы содержится практическое решение поставленной проблемы формирования кибербезопасности студентов ПОО и экспериментальная апробация предлагаемых материалов.

В данной главе раскрываются ответы на следующие вопросы:

1) Описание базы исследования, а именно описана информационная среда профессиональной образовательной организации ГБПОУ «Южно-Уральский государственный технический колледж» как фактор формирования основ кибербезопасности у студентов ПОО.

2) Формирующий этап эксперимента, а именно мероприятия по формированию основ кибербезопасности.

3) Экспериментальная проверка комплекса мероприятий, получение и анализ результатов констатирующего этапа для подтверждения или опровержения гипотезы.

Результаты педагогического эксперимента, описанные в главе 2, являются подтверждением того, что разработанный комплекс мероприятий действительно развивает основы кибербезопасности у студентов профессиональной образовательной организации в процессе подготовки специалистов среднего звена на примере ГБПОУ «Южно-Уральский государственный технический колледж», эффективность эксперимента была доказана методом математической статистики, а именно t-критерием Стьюдента.

В результате педагогического эксперимента, удалось прийти к выводу, что предложенный комплекс мероприятий обучения основам кибербезопасности, результативен. Гипотеза, выдвинутая в выпускной квалификационной работе, подтверждена.

ЗАКЛЮЧЕНИЕ

Цифровая грамотность действительно играет ключевую роль в подготовке специалистов среднего звена, помогая им успешно ориентироваться в современном информационном пространстве и эффективно использовать цифровые технологии. Однако важно учитывать не только положительные, но и возможные негативные последствия, связанные с развитием цифровой грамотности.

В данной выпускной квалификационной работе мы ответили на вопрос, почему так важно включать элементы обучения кибербезопасности в образовательный процесс.

Во – первых, это защита личных данных. Студенты должны осознавать риски, связанных с утечкой личной информации, и знать способы её защиты (использование антивирусов, сложные пароли, двухфакторная аутентификация). Именно это поможет выпускникам профессиональной образовательной организации предотвратить возможные потери в дальнейшей профессиональной и личной жизнедеятельности.

Во – вторых, это противодействие кибербуллингу. Студенты и выпускники профессиональных образовательных организаций обязаны понимать природу кибербуллинга и его последствия, а также умело адекватно реагировать на агрессию в интернете, это поможет снизить вероятность попадания в неприятные ситуации.

В – третьих, это контроль времени и ресурсов. Именно обучение управлению временем и ресурсами в цифровом пространстве помогает избежать зависимости от гаджетов и сохранять баланс между работой и отдыхом.

В – четвертых, этические нормы в интернете. Изучение правил поведения в интернете и этических норм помогает пользователям вести себя ответственно и уважительно по отношению к другим людям.

Правильно построенное обсуждение технологических, правовых, психологических, нравственных, медицинских аспектов информационной безопасности на уроках общеобразовательной учебной дисциплины Информатика, на классных часах и учебных занятиях, во время аудиторной и внеаудиторной работы вызывает интерес у студентов, способствует формированию стремления осмыслить факторы риска, характер влияния этих факторов риска на человека и общество, студенты получают представление о средствах и способах защиты, а также вырабатывают собственное отношение к факторам риска информационного общества, что формирует кибербезопасность.

Действительно, большинство студентов, приходящих в профессиональные образовательные организации, уже обладают определённым опытом использования компьютерных игр и Интернета. Это создаёт как возможности, так и вызовы для образовательного процесса. Воспитательная и обучающая работа, основанная на педагогических закономерностях, направлена на подготовку студентов к ответственному и безопасному взаимодействию с информационными технологиями.

Студенты, как правило, хорошо знакомы с компьютерами, мобильными устройствами и социальными сетями. Они проводят много времени в играх и интернете, что может иметь как позитивные, так и негативные последствия. С одной стороны, это даёт им определённые технические навыки, с другой – может приводить к зависимостям, отвлечению от учёбы и проблемам с кибербезопасностью.

Коррекция негативных тенденций возможна только при условии сотрудничества всех участников образовательного процесса. Преподаватели, родители и сами студенты должны работать вместе, чтобы создавать здоровую и безопасную цифровую среду.

Только так можно подготовить студентов и выпускников ПОО к успешным и безопасным встречам с информационными факторами риска.

Положительное влияние педагогического процесса на информационную безопасность студентов действительно усиливается, когда они получают знания о различных аспектах влияния информационных технологий на личность и общество. Вот как эти знания могут способствовать укреплению кибербезопасности:

1) Влияние уровня информационной безопасности на реализацию потребностей. Когда студенты понимают, как уровень их собственной информационной безопасности влияет на способность реализовать свои актуальные потребности, они становятся более осознанными пользователями цифровых технологий. Например:

– личная жизнь. Безопасность личных данных защищает частную жизнь студента, выпускника и в дальнейшем специалиста и предотвращает вмешательство третьих лиц;

– профессиональное развитие. Надежная информационная среда способствует эффективному обучению и профессиональному росту;

– экономическая стабильность. Знание о защите финансовых данных снижает риск финансовых потерь и мошенничества.

2) Деструктивные социальные группы. Осведомленность о существовании деструктивных социальных групп, стремящихся оказать негативное влияние на человека посредством информационных технологий, помогает студентам быть более осторожными и критичными в восприятии информации. Это включает:

– кибербуллинг. Понимание опасности агрессивного поведения в интернете и умение распознавать манипулятивные техники;

– радикализация. Знания о методах вербовки в экстремистские группировки и как противостоять такому давлению;

– финансовые пирамиды и мошеннические схемы. Осознанность в отношении различных видов финансового мошенничества в интернете.

3. Экономика компьютерных игр. Компьютерные игры представляют собой не только развлекательный продукт, но и важную часть современной

экономики. Игровая индустрия – это многомиллиардный рынок с множеством аспектов, которые влияют как на игроков, так и на компании-разработчиков. Понимание экономической мотивации создателей компьютерных игр помогает студентам осознать, что такие игры могут быть разработаны с целью извлечения прибыли любой ценой, даже если это негативно сказывается на пользователях. Это знание побуждает студентов к более критичному восприятию контента и выбору игр, соответствующих их ценностям и интересам, формирует критическое мышление.

Комплексный подход к обучению информационной безопасности, включающий вышеперечисленные аспекты, способствует формированию у студентов осознанного и ответственного отношения к использованию цифровых технологий. Это, в свою очередь, укрепляет их устойчивость к внешним угрозам и помогает минимизировать риски, связанные с информационными факторами.

Демонстрация примеров успешных действий специалистов в области кибербезопасности действительно может оказывать значительное влияние на формирование мотивации у студентов. Когда студенты узнают о реальных примерах работы экспертов, правоохранителей и программистов, они начинают лучше понимать важность и сложность информационной безопасности, а также осознавать, какую роль они могут сыграть в обеспечении безопасности в цифровом пространстве.

Истории успехов специалистов в области кибербезопасности показывают студентам, что их усилия могут принести реальную пользу обществу, а знание о том, что специалисты по кибербезопасности востребованы и высоко оплачиваемы, может стимулировать стремление к приобретению соответствующих навыков. Это помогает им осознавать важность и значимость своей и других специальностей, стремиться к достижению высоких результатов в профессиональной сфере и жизни в современном информационном пространстве.

Элементы новизны исследования заключаются в том, что был разработан комплекс мероприятий для формирования основ кибербезопасности обучающихся профессиональной образовательной организации.

В процессе написания выпускной квалификационной работы был проведен педагогический эксперимент, целью которого было подтвердить или опровергнуть гипотезу: формирование основ кибербезопасности будет более эффективным, если выявить и реализовать комплекс мероприятий по формированию основ кибербезопасности у студентов профессиональной образовательной организации.

Результаты педагогического эксперимента показали, что комплекс мероприятий при преподавании общеобразовательной учебной дисциплины Информатика действительно развивает основы кибербезопасности студентов профессиональной образовательной организации на примере ГБПОУ «Южно-Уральский государственный технический колледж», что было подтверждено с помощью метода математической статистики, а именно с помощью метода t-критерия Стьюдента.

Гипотеза исследования, а именно: формирование основ кибербезопасности у студентов профессиональной образовательной организации будет более эффективным, если выявить и реализовать комплекс мероприятий по основам кибербезопасности, была подтверждена.

Основные задачи исследования в части систематизации теоретических основ кибербезопасности, изучения информационной среды профессиональной образовательной организации, разработке и экспериментальной проверке комплекса мероприятий по формированию основ кибербезопасности обучающихся профессиональной образовательной организации на примере ГБПОУ «Южно-Уральский государственный технический колледж», решены.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Конституция Российской Федерации / Принята на всенародном голосовании 12 декабря 1993 г. [Электронный ресурс]. - Режим доступа: http://constitution.kremlin.ru/.(Дата обращения: 15.10.2024)
2. Закон РФ от 21 июля 1993 №5485-1 «О государственной тайне (с изменениями на 8 августа 2024 года)» [Электронный ресурс]. - Режим доступа: https://docs.cntd.ru/document/9004687?section=text (Дата обращения: 15.10.2024)
3. Концепция стратегии кибербезопасности Российской Федерации. Проект [Электронный ресурс].– Режим доступа: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (Дата обращения: 15.10.2024)
4. Приказ Министерства образования и науки Российской Федерации от 17 мая 2012 г. № 413 «Об утверждении федерального государственного образовательного стандарта среднего общего образования (с изменениями на 27 декабря 2023 года)» [Электронный ресурс].– Режим доступа: https://docs.cntd.ru/document/902350579?section=text (Дата обращения: 04.11.2024).
5. Распоряжение Правительства Российской Федерации от 28 апреля 2023 г. № 1105-р «Концепция информационной безопасности детей в Российской Федерации» [Электронный ресурс]. – 2023. – Режим доступа: http://static.government.ru/media/files/0vjjsdBmSsIdUZ4c8Z2eOAiGkCbCf7OJ.pdf (Дата обращения: 14.10.2024).
6. Указ Президента Российской Федерации от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» [Электронный ресурс].– Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202104120050 (Дата обращения: 15.10.2024)

7. Указ Президента РФ от 05 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»: [Электронный ресурс]. – 2020. – Режим доступа: http://static. kremlin.ru/media/acts/files/ 0001201612060002.pdf (Дата обращения: 14.04.2024).
8. Указ Президента РФ от 09 мая 2017 г. №203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы [Электронный ресурс].– Режим доступа: http://static.kremlin.ru/media/acts/files/0001201705100002.pdf (Дата обращения: 15.10.2024)
9. Федеральный закон от 24 июля 1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации (с изменениями на 23 ноября 2024 года) [Электронный ресурс]. – 2020. – Режим доступа: https://docs.cntd.ru/document/901713538?section=text (Дата обращения: 15.12.2024)
10. Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями на 23 ноября 2024 года) // Профессиональные справочные системы «Кодекс» и Техэксперт». [Электронный ресурс].– Режим доступа: https://docs.cntd.ru/document/901990051?section=text (Дата обращения: 14.04.2024)
11. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» (В редакции федеральных законов от 05.10.2015 № 285-ФЗ, от 06.02.2020 № 6-ФЗ, от 09.11.2020 № 365-ФЗ, от 28.04.2023 № 155-ФЗ, от 10.07.2023 № 286-ФЗ): [Электронный ресурс]. – 2024. – Режим доступа: http://www.kremlin.ru/acts/bank/32417(Дата обращения: 15.10.2024)
12. Федеральный закон от 29 декабря 2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» [Электронный ресурс]. – 2020. – Режим доступа: http://www.kremlin.ru/acts/bank/32492 (Дата обращения: 15.10.2024)

13. Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации (с изменениями на 13 декабря 2024 года) (редакция, действующая с 24 декабря 2024 года)» [Электронный ресурс].– Режим доступа: https://docs.cntd.ru/document/902389617?section=text (Дата обращения: 15.10.2024)
14. Федеральный партийный проект «Цифровая Россия» [Электронный ресурс].– Режим доступа: https://digital.er.ru/ (Дата обращения: 15.11.2024)
15. Федеральный проект «Молодые профессионалы» [Электронный ресурс].– Режим доступа: https://edu.gov.ru/national-project/projects/professionals/(Дата обращения: 15.11.2024)
16. Федеральный проект «Профессионалитет» [Электронный ресурс].– Режим доступа: https://edu.gov.ru/activity/main_activities/additional_vocational_education/ (Дата обращения: 15.12.2024)
17. Федеральный проект «Цифровая образовательная среда» [Электронный ресурс].– Режим доступа: https://edu.gov.ru/national-project/projects/cos/ https://edu.gov.ru/national-project/projects/cos/(Дата обращения: 15.12.2024)
18. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Официальное издание. М.: Стандартинформ, 2018 год. [Электронный ресурс]. 2020. – Режим доступа: https://docs.cntd.ru/document/1200075565?section=text(Дата обращения: 04.10.2024).
19. ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели: – 2020. [Электронный ресурс].– Режим доступа: https://docs.cntd.ru/document/1200114169?section=text (Дата обращения: 04.10.2024).

20. Артемов, А.В. Информационная безопасность: курс лекций / А.В.Артемов; Межрегиональная Академия безопасности и выживания. – Орел: МАБИВ, 2014. - 257 с. [Электронный ресурс].– Режим доступа: http://www.litres.ru/pages/biblio_book/?art=9066361 (Дата обращения: 16.10.2024).
21. Безкоровайный М.М., Татузов А.Л. Кибербезопасность подходы к определению понятия // Вопросы кибербезопасности. 2014. №1 (2). [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/ article/n/kiberbezopasnost-podhody-k-opredeleniyu-ponyatiya (дата обращения: 22.11.2024).
22. Бессонова, А.В. Организация и результаты внедрения методики обучения информатике на примере раздела «Логические основы компьютеров» на основе семиотического подхода. Российский государственный профессионально-педагогический университет (филиал) в г. Нижнем Тагиле, Россия. [Электронный ресурс]. – Режим доступа: https://s.eduherald.ru/pdf/2021/1/20405.pdf(Дата обращения: 16.11.2024).
23. Вигриянова, Ю.С. Реконструкция модели кибербезопасности в российских банках (на примере ПАО «Сбербанк России») [текст]: автореферат магистерской диссертации / Вигриянова Ю.С. – Екатеринбург, 2020 [Электронный ресурс]. – Режим доступа: https://elar.urfu.ru/bitstream/10995/86553/1/m_th_y.s.vigriyanova_2020.pdf(Дата обращения: 16.11.2024).
24. Вострецова, Е.В. Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург: Изд-во Урал. ун-та, 2019.— 204 с. [Электронный ресурс]. – Режим доступа: https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf
25. Всероссийский образовательный проект в сфере цифровой экономики Урок цифры [Электронный ресурс]. – Режим доступа: https://урокцифры.рф/ (Дата обращения: 16.11.2024).

26. Всероссийский проект «Цифровой Диктант» [Электронный ресурс]. – Режим доступа: https://digitaldictation.ru/ (Дата обращения: 14.04.2024).
27. ВТБ Онлайн Против мошенников [Электронный ресурс]. – Режим доступа: https://digest.vtb.promo/safety?code=media_tg_scammers&utm_source=tg&utm_medium=media&utm_campaign=media_scammers_tg_mash_cpv_rf_p3_dec&erid=2VtzqwzUrnc(Дата обращения: 16.11.2024).
28. Дерендяева Н.С. Структура, критерии, уровни и показатели сформированности культуры информационной безопасности школьников // Наука и школа. 2016. №5. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/struktura-kriterii-urovni-i-pokazateli-sformirovannosti-kultury-informatsionnoy-bezopasnosti-shkolnikov (Дата обращения: 17.11.2024).
29. Диденко Е.В., Гафарова Е.А., Степанова О.А. Анализ результатов экспериментальной работы по формированию готовности обучающихся колледжа к противодействию вовлечения в киберэкстремистскую деятельность/ Диденко Г.А., Шамаева Т.Н. . – Челябинск: ФГБОУ ВО «Южно-Уральский государственный гуманитарно-педагогический университет». [Электронный ресурс]. – Режим доступа: https://s.top-technologies.ru/pdf/2019/8/37640.pdf (Дата обращения: 04.10.2024).
30. Кибербезопасность для детей и взрослых //Государственная образовательная платформа «Российская электронная школа» [Электронный ресурс]. – Режим доступа: https://resh.edu.ru/page/cyber-project (Дата обращения: 16.11.2024).
31. Кибербезопасность от А до Я// ПАО «Софтлайн». [Электронный ресурс]. – Режим доступа: https://softline.ru/about/blog/kiberbezopasnost-ot-a-do-ya (Дата обращения: 15.10.2024)
32. КиберКвиз Первых в рамках проекта «Азбука кибербезопасности». [Электронный ресурс]. – Режим доступа: https://будьвдвижении.рф/projects/2387(Дата обращения: 15.11.2024)

33. Коваленко, Ю. И., Методика защиты информации в организациях: монография / Ю. И. Коваленко, Г. И. Москвитин, М. М. Тараскин. — Москва : Русайнс, 2020. — 162 с. — ISBN 978-5-4365-0887-0. — URL: https://book.ru/book/934719 (дата обращения: 09.11.2024). — Текст : электронный.
34. Козлова Н.Ш., Довгаль В.А Кибербезопасность и информационная безопасность: сходства и отличия // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2021. №3 (286). [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/kiberbezopasnost-i-informatsionnaya-bezopasnost-shodstva-i-otlichiya (Дата обращения: 20.10.2024).
35. Лига безопасного Интернета [Электронный ресурс]. – Режим доступа: https://ligainternet.ru/vserossijskij-urok-bezopasnogo-interneta/(Дата обращения: 16.10.2024).
36. Макаров С. Прекрасный, опасный, кибербезопасный мир. Всё, что важно знать детям и взрослым о безопасности в интернете – М.: Ростелеком. 2022. – 568 с.: ил. [Электронный ресурс]. – Режим доступа: https://www.company.rt.ru/social/cyberknowledge/book_cybersecurity/ (Дата обращения: 16.11.2024).
37. Математические методы обработки данных [Электронный ресурс]. – Режим доступа: https://www.psychol-ok.ru/lib/statistics.html (Дата обращения: 20.11.2024).
38. Медийная и информационная грамотность: программа обучения педагогов. – М.: Институт ЮНЕСКО по информационным технологиям в образовании, 2012. [Электронный ресурс]. – Режим доступа: https://unesdoc.unesco.org/ark:/48223/pf0000192971_rus (Дата обращения: 20.11.2024).
39. Меры безопасности при работе с приложениями и сервисам Сбербанка [Электронный ресурс]. – Режим доступа: https://sber-

info.ru/merybezopasnosti-pri-rabote-s-prilozheniyami-i-servisam-sberbanka/(Дата обращения: 15.10.2024)

40. Олимпиада «Безопасный интернет» [Электронный ресурс]. – Режим доступа: Учи.ру(Дата обращения: 14.12.2024).
41. Онлайн-викторина «Безопасное поведение в сети Интернет»// Центр правовой информации [Электронный ресурс]. – Режим доступа: https://wordwall.net/play/25815/361/907 (Дата обращения: 14.04.2024).
42. Осведомленность о кибербезопасности//компания Майкрософт: [Электронный ресурс]. – Режим доступа: https://www.microsoft.com/ru-ru/security/business/cybersecurity-awareness (Дата обращения: 14.04.2024).
43. Петров П.К. Математико-статистическая обработка и графическое представление результатов педагогических исследований с использованием информационных технологий: учеб. Пособие / П.К. Петров. – 2-е изд., исправ., и доп. – Ижевск: Издательский центр «Удмуртский университет», 2016. – 176 с
44. Подласый, И. П. Педагогика: учебник для вузов / И. П. Подласый. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2024. — 575 с. — (Высшее образование). — ISBN 978-5-534-03772-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/535418 (дата обращения: 02.12.2025).
45. Примерная основная образовательная программа среднего общего образования. Одобрена решением федерального учебно-методического объединения по общему образованию (протокол от 28 июня 2016 г. № 2/16-з) – 2023. [Электронный ресурс].– Режим доступа: https://fgosreestr.ru/poop/primernaya-osnovnaya-obrazovatelnaya-programma-srednego-obshhego-obrazovaniya (Дата обращения: 14.04.2024).
46. Рубцова О.В. Риски в цифровой среде: диагностика, профилактика, коррекция: учебно-методическое пособие / Московский

государственный психолого-педагогический университет; под ред. О.В. Рубцовой, Е.М. Шпагиной, А.А. Шведовской, Н.В. Дворянчикова.– М: МГППУ. – 2024. 152 с. [Электронный ресурс].– Режим доступа: https://gppc.ru/wp-content/uploads/2024/12/riski-v-czifrovoj-srede.pdf(Дата обращения: 14.04.2024).

47. Селиванова О. В., Иванова И. Ю., Примакова Е. А., Кривопалова И. Методические рекомендации: Методика организации недели «Безопасность Интернет»./Авторы составители: Селиванова О. В., Иванова И. Ю., Примакова Е. А., Кривопалова И. .Тамбов, ИПКРО 2015. [Электронный ресурс]. – Режим доступа: https://gymn116.ru/pdf/%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F/teach/metod%20nedelya-internet.pdf (Дата обращения: 14.12.2024).
48. Система дистанционного обучения ГБПОУ «Южно-Уральский государственный технический колледж» [Электронный ресурс]. – Режим доступа: dom.sustec.ru (Дата обращения: 14.04.2024).
49. Серёдкин С.П. Современный взгляд на толкование понятия кибербезопасность – г. Иркутск: Иркутский государственный университет путей сообщения [Электронный ресурс]. – Режим доступа: Режим доступа: https://ismm.irgups.ru/sites/default/files/articles_pdf_files/modern_ view.pdf (Дата обращения: 16.12.2024).
50. Смирнов В.М., Чернякова Е.М. Право ребенка на кибербезопасность // StudNet. 2022. №3. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/pravo-rebenka-na-kiberbezopasnost (Дата обращения: 15.12.2024).
51. Столбов П. А. Состояние информационной безопасности в Российской Федерации // Вестник науки. 2024. №6 (75). [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/sostoyanie-

informatsionnoy-bezopasnosti-v-rossiyskoy-federatsii (Дата обращения: 15.12.2024).

52. Тимофеева Л.Л. Методические рекомендации по обеспечению информационной безопасности в образовательной организации / сост. Л. Л. Тимофеева. – Орёл: Бюджетное учреждение Орловской области дополнительного профессионального образования «Институт развития образования», 2020. – 58. с.– Текст: непосредственный. [Электронный ресурс]. – Режим доступа: https://xn--h1albh.xn--p1ai/wp-content/uploads/2021/06/Metodicheskie-rekomendacii-po-obespecheniju-informacionnoj-bezopasnosti-v-obrazovatelnoj-organizacii.pdf (Дата обращения: 15.12.2024).
53. Уроки безопасности в школе (КИБЕРуроки). Сборник методических разработок. – Пермь: Муниципальное бюджетное учреждения «Центр психолого-педагогической, медицинской и социальной помощи» [Электронный ресурс]. – Режим доступа: https://xn--l1afhav.xn--p1ai/files/biblioteka/%D0%9A%D0%98%D0%91%D0%95%D0%A0%D0%A3%D0%A0%D0%9E%D0%9A%D0%98_2022_%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5_%D1%80%D0%B0%D0%B7%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%BA%D0%B8.pdf (Дата обращения: 15.12.2024).
54. Что такое безопасность [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security(Дата обращения: 16.11.2024).
55. Электронная библиотека и интернет-магазин учебной и научной литературы Знаниум [Электронный ресурс]. – Режим доступа: https://znanium.ru/(Дата обращения: 16.12.2024).
56. Южно-Уральский государственный технический колледж [Электронный ресурс]. – Режим доступа: sustec.ru (Дата обращения: 04.10.2024).

57. Яковлева Н.О. Концепция педагогического проектирования: методологические аспекты: Монография. – М: Информационно-издательский центр АТиСО, 2002. – 194 с. [Электронный ресурс]. – Режим доступа: http://elib.cspu.ru/xmlui/bitstream/handle/123456789/276/%D0%9A%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%86%D0%B8%D1%8F%20%D0%BF%D1%80%D0%BE%D0%B5%D0%BA%D1%82%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F%202002.pdf?sequence=1&isAllowed=y (Дата обращения: 16.12.2024).
58. ИСО/МЭК 27032:2023 Кибербезопасность – Руководство по безопасности в Интернете [Электронный ресурс]. – Режим доступа: https://www.iso.org/standard/76070.html (Дата обращения: 16.12.2024).
59. Moodle – система управления образовательными электронными курсами [Электронный ресурс]. – Режим доступа: moodle.org (Дата обращения: 04.10.2024).
60. NIST. Национальный институт стандартов и технологий США [Электронный ресурс]. – Режим доступа: https://www.nist.gov/cybersecurity (Дата обращения: 04.10.2024).
61. Positive Technologies [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/(Дата обращения: 07.12.2024).

ПРИЛОЖЕНИЕ

Приложение 1

КИБЕРУРОК «БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ: ПРАВИЛА БЕЗОПАСНОЙ РАБОТЫ В СЕТИ»

Цель: знакомство с правилами безопасной работы в сети Интернет.

Задачи:

- изучить информированность пользователей о безопасной работе в сети Интернет;
- познакомить с правилами безопасной работы в Интернете;
- учить ориентироваться в информационном пространстве;
- способствовать ответственному использованию online-технологий;
- формировать информационную культуру студентов;
- умение самостоятельно находить нужную информацию пользуясь web-ресурсами;
- развивать критическое мышление;
- воспитывать дисциплинированность при работе в сети.

Обучающиеся должны знать:

- перечень информационных услуг сети Интернет;
- опасности глобальной компьютерной сети.

Учащиеся должны уметь:

- работать с Web-браузером;
- пользоваться информационными ресурсами;
- искать информацию в сети Интернет;
- ответственно относиться к использованию online-технологий.

Тип урока: урок изучения нового материала

Методы и формы обучения: словесный (дискуссия, рассказ), видеометод, наглядный (демонстрация), практический; частично-поисковый, проблемный, метод мотивации интереса; интерактивная форма обучения (обмен мнениями, информацией).

Программно-дидактическое обеспечение: презентация «Безопасный Интернет.pptx», видеофайлы «Дети и Интернет.flv», «Учите детей общаться.flv», тест, информационные плакаты, карточки с адресами Web-ресурсов.

Этапы урока:

1. Организация начала урока. Постановка цели урока. Просмотр видеоролика. Постановка темы и главного вопроса урока.
2. Изучение нового материала. Дискуссия в группе. Теоретическое освещение вопроса (сообщения обучающихся).
3. Практическая работа. Поиск информации в сети Интернет. Дискуссия по найденному материалу.
4. Закрепление изученного материала. Рекомендации по правилам безопасной работы. Тестирование.
5. Подведение итогов урока. Оценка работы группы. Просмотр видеоролика. Информация о домашнем задании.

Ход урока

1. Организация начала урока. Постановка цели урока (3 мин). Развитие глобальной сети изменило наш привычный образ жизни, расширило границы наших знаний и опыта. Теперь у вас появилась возможность доступа практически к любой информации, хранящейся на миллионах компьютерах во всём мире. Но с другой стороны, миллионы компьютеров получи доступ к вашему компьютеру. И не сомневайтесь, они воспользуются этой возможностью. И не когда-то, а прямо сейчас.

– Внимание, видеоролик! (Просмотр видеоролика «Дети и Интернет» – 1 мин.)

– Как не стать жертвой сети Интернет? Тема нашего урока - «Безопасный Интернет». Главный вопрос урока: Как сделать работу в сети безопасной?

2. Изучение нового материала (18 мин). Игра «За или против» (5 мин.).

Для начала, предлагаю поиграть в игру «За или против». Вы увидите несколько высказываний. Попробуйте привести аргументы, отражающие противоположную точку зрения.

– Интернет имеет неограниченные возможности дистанционного образования. И этохорошо!

– Интернет – это глобальный рекламный ресурс. И это хорошо!

– Общение в Интернете – это плохо, потому что очень часто подменяет реальное общение виртуальному.

– Интернет магазины – это плохо, потому что это наиболее популярный вид жульничества в Интернете.

– В Интернете можно узнать сведения о человеке (место проживания и адрес электронной почты, номер мобильного телефона). И это хорошо!

Виртуальные грабли (8 мин.)

– Какие опасности подстерегают нас? Какие виртуальные грабли лежат у нас на пути? Посмотрим, что на это скажет Таня, которая подробно познакомилась с этой проблемой дома (сообщение студента по темам: «Интернет-зависимость», «Вредоносные и нежелательные программы», «Онлайновое пиратство»).

– Как уберечься от недостоверной информации? Кто такие интернет-мошенники? Расскажет Владимир (сообщение студента по темам: «Как уберечься от недостоверной информации?», «Материалы нежелательного содержания», «Интернет-мошенники»).

– Общение в Интернете. Какое оно? Послушаем Марию (сообщение студента по теме «Преступники в Интернете», «Интернет-дневники»).

Физ. минутка «Собери рукопожатия» (2 мин.).

Участникам предлагается в течение 10 секунд пожать руки как можно большего числа других людей.

Обсуждение. Кому сколько человек удалось поприветствовать? У кого-то возник психологический дискомфорт? Чем он был вызван?

Аналогия с работой в Интернет. Общаясь в Интернете, мы очень часто добавляем незнакомых людей в свои социальные сети и общаемся с ними. Мы не знаем про них ничего, только их Ники. Как много информации про человека мы можем узнать от Ника или рукопожатия?

Ответим на главный вопрос урока – «Как сделать работу в сети безопасной?»

3. Практическая работа (7 мин.).

– Что можно? Что нельзя? К чему надо относиться осторожно? Давайте посмотрим, что об этом можно прочитать на web-страницах и попробуем сформулировать правила безопасной работы.
– У вас на столах лежат карточки с адресами web-страниц, которые я предлагаю вам сегодня посетить. Данный ресурс добавлен в закладки браузера Opera в папку «Безопасный Интернет». Познакомьтесь с информацией ресурса и сформулируйте правила безопасной работы в сети.

Резюмируем (обсуждение найденной информации). Какие правила безопасной работы вы выбрали, посещая web-сайты?

4. Закрепление изученного материала (12 мин). Я тоже для вас приготовила несколько советов. Интернет – это новая среда взаимодействия людей. В ней новое звучание приобретают многие правила и закономерности, известные людям с давних времен. Попробую сформулировать некоторые простые рекомендации, используя хорошо известные образы.

Повернись, избушка, ко мне передом, а к лесу задом! Современный Интернет – это не только обширная, но и настраиваемая среда обитания! В нем хорошо тому, кто может обустроить в нем собственное пространство и научиться управлять им. Записывайте свои впечатления в блог, создавайте галереи своих фотографий и видео, включайте в друзья людей, которым вы доверяете. Тогда вместо бессмысленного блуждания по сети ваше Интернет общение будет приносить пользу.

Не пей из колодца! Даже когда мы испытываем жажду, мы не будем пить из грязной лужи. Также и в среде Интернет, случайно оказавшись в месте, которое производит отталкивающее впечатление агрессивного и замусоренного, лучше покинуть его, переборов чувство любопытства. Это защитит вас от негативных эмоций, а ваш компьютер – от вредоносного программного обеспечения.

Волку дверь не открывайте! У интернет-мошенников ничего не получится, если только мы сами не откроем им дверь – не сообщим им наши пароли, не загрузим на свой компьютер сомнительные файлы или не дадим возможность пользоваться нашей сетью незнакомым людям.

5. Подведение итогов урока (5 мин.).

Я рада, что вы не остались равнодушны к теме безопасного интернета. Спасибо за активное участие (оценка работы группы). Каждый год, проходит День безопасного Интернета. Его цель – способствовать безопасному и более ответственному использованию онлайн-технологий и мобильных телефонов среди детей и молодежи по всему миру. Впервые он проводился в 2004 году, и с тех пор число его участников постоянно растет. Для его проведения был образован Российский Оргкомитет, в состав которого вошли представители практически всех ведущих общественных, некоммерческих и других организаций, деятельность которых связана с развитием Интернета. В рамках проведения Дня безопасного Интернета прошел конкурс на лучший видеоролик. Ролик, занявший 1 место, вы видели в начале урока. - В завершении нашего урока предлагаю посмотреть еще одну интересную конкурсную работу (просмотр видеоролика «Учите детей общаться.pptx» - 0, 35 сек.)

Приложение 2

ОНЛАЙН-ВИКТОРИНА «БЕЗОПАСНОЕ ПОВЕДЕНИЕ В СЕТИ ИНТЕРНЕТ»

Интернет-безопасность – это безопасность действий и транзакций, совершаемых в интернете. Интернет-безопасность входит в более широкие понятия, такие как кибербезопасность и компьютерная безопасность, и включает безопасность браузера и сети, а также правильное поведение в сети. Проводя значительное время в сети, можно столкнуться со следующими угрозами интернет-безопасности:

Взлом – получение неавторизованными пользователями доступа к компьютерным системам, учетным записям электронной почты и веб-сайтам.

Вирусы и вредоносные программы, которые могут повредить данные и сделать системы уязвимыми для других угроз.

Кража личных данных, например, личной и финансовой информации злоумышленниками.

Чтобы сохранить конфиденциальность и безопасность в интернете, важно знать о различных типах интернет-атак. Ниже описаны распространенные угрозы интернет-безопасности.

Чтобы обеспечить безопасность в интернете и защитить свои данные, можно следовать перечисленным ниже рекомендациям.

Используйте многофакторную аутентификацию везде, где возможно.

Используйте сетевой экран (Сетевые экраны блокируют нежелательный трафик, а также помогают предотвратить заражение компьютера вредоносными программами)

Внимательно относитесь к выбору браузера.

Создавайте надежные пароли и используйте менеджер паролей.

Надежный пароль помогает обеспечить безопасность в интернете. Он обладает следующими свойствами:

Длинный: минимум 12 символов, в идеале, даже больше.

Содержит заглавные и строчные буквы, а также специальные символы и цифры.

Не очевидный: в пароле не используются комбинации последовательных цифр (1234) и личная информация, которую может угадать тот, кто вас знает, например, дата рождения или имя домашнего животного.

Не содержит запоминающихся сочетаний клавиш.

Используйте на устройствах последнюю версию программы безопасности.

Викторина «Безопасное поведение в сети Интернет», подготовленная Центром правовой информации поможет Вам проверить свои знания в области информационной безопасности. Ссылка https://wordwall.net/play/25815/361/907

Приложение 3

КВИЗ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель квиза: Познакомиться с информационной безопасностью и возможными способами применения современных методов и средств защиты информационных ресурсов, персональных данных.

Задачи: Выявить проблемы информационной и кибербезопасности и сформировать культуру обращения с персональными данными.

Ожидаемые результаты: Повышение уровня кибербезопасности. Условия: Регистрация на мероприятии через систему дополнительного образования Московской области.

Ход мероприятия:

Еще недавно мы вносили паспортные данные и другую личную информацию где и когда угодно: для розыгрыша мгновенной лотереи, для получения скидочной карты, и много где еще. Реалии современного информационного общества диктуют новые требования к безопасности персональных данных, а так же выявляют необходимость формирования культуры обращения с информацией. Наш КВИЗ поможет в этом разобраться. В чем суть КВИЗА? Вы набираете баллы за правильные ответы на вопросы. Вопросы имеют разную сложность и приносят разное количество баллов. Время ответа на каждый вопрос не ограничено. После ответа на все вопросы Вы узнаете количество набранных баллов и получите сертификат. Это будет полезно? Вопросы построены на основе анализа наиболее распространённых ошибок людей, использующих сеть Интернет. КВИЗ поможет понять, какие ситуации представляют для Вас потенциальную опасность.

ПЛАН. Для того чтобы пройти наш КВИЗ «Что вы знаете об информационной безопасности?» скорее нажимай на ссылку или копируй её в адресную строку и начинай выполнять задания. Тебе точно понравится. https://forms.yandex.ru/u/65493d3d3e9d089a7fb59542/

Приложение 4

ЦИКЛ УЧЕБНЫХ ЗАНЯТИЙ ПО КИБЕРБЕЗОПАСНОСТИ «УДИВИТЕЛЬНЫЙ И ОПАСНЫЙ МИР ИНТЕРНЕТА»

Занятие 1 «Опасности сети Интернет» (50-55 минут)

Цель: Актуализация знаний студентов о различных Интернет-опасностях, предупреждение формирования Интернет-зависимости у подростков.

Задачи:

1. Уточнить представления подростков об Интернет-опасностях.
2. Способствовать осознанию различных Интернет-опасностей и рисков Интернет-зависимости.
3. Оказать помощь в снятии психоэмоционального напряжения.
4. Воспитывать умение аргументировать своё мнение.
5. Развивать у студентов чувство ответственности за свое здоровье.
6. Способствовать осознанию подростками своих ценностей.

Материалы: листы, цветные карандаши (фломастеры), классная доска (маркерная доска), презентация «Безопасный Интернет», проектор, опорные слова для рефлексии, символы правил поведения на занятии (или листы для изготовления символов по ходу занятия), цветные листы бумаги или картона для обозначения 4-х углов.

Ход занятия

1. Приветствие, психологический настрой. Упражнение «Статус» (5 минут) Каждому участнику предлагается озвучить свой «сетевой статус» - предложение, обозначающее его эмоциональное состояние на данный момент. Это может быть цитата из книги, стихотворение или просто описание того, что подросток чувствует в данный момент.

2. Знакомство с правилами поведения на занятии (3 минуты). Примерные формулировки правил поведения на занятии:

«можно»:

- не вставать с места при ответе;
- высказывать любое своё мнение и отстаивать его;

– уважать мнение своих товарищей;

– не бояться ошибиться, так как каждый человек имеет право на ошибку;

– помогать своему товарищу

«нельзя»:

– перебивать говорящего товарища, выкрикивать с места;

– смеяться над чужим мнением;

– смеяться над ошибками. И другие.

Правила формулируются самими учащимися, рисуются символы.

Разминка. Упражнение «Четыре угла» (5 минут) Участникам предлагается обсудить, какие положительные или негативные моменты Интернет привносит в нашу жизнь. Предлагается выбрать один из четырёх углов в зависимости от мнения и аргументировать своё мнение.

1. Красный угол – становятся те, кто считает, что Интернет приносит только пользу.

2. Чёрный угол выбирают те, кто считает, что Интернет приносит много вреда.

3. Зелёный угол – больше пользы, чем вреда (обозначить параметры пользы и вреда).

4. Оранжевый угол – больше вреда, чем пользы (обозначить параметры пользы и вреда).

Аргументируем ответы каждой группы

4. Информационный блок. Групповая дискуссия (10 минут)

Сейчас, вероятно, нет такого человека, который пользовался интернетом и не был бы зарегистрирован на каком-либо сайте. Каждый ребёнок играет в компьютерные игры, выполняет задания по учебным предметам, общается в социальных сетях.

Ведущий предлагает участникам разделиться на две группы: первая – приводит доводы, что человек не может сделать без компьютера, а вторая – что компьютер не может дать человеку. Каждая группа четко

аргументирует свою точку зрения, приводит примеры. В процессе обсуждения оппоненты не только настаивают на своем, но и опровергают мнение соперника.

Рефлексия:

– Какие чувства вы испытывали во время выполнения упражнения?
– Трудно ли было отстаивать свое мнение? Что для себя открыли?

Ведущий: Давайте подумаем, есть ли у компьютерных игр положительные стороны? Отрицательные? Какие? (ответы студентов)
(Подсказка)
Положительные стороны компьютерных игр

– логические и обучающие игры; учат детей счету, иностранному алфавиту;

– интересное развлечение и способ занять свое свободное время;

– возможность стать главным героем игрового пространства, что нереализуемо в обычном мире;

– общение с другими игроками (в многопользовательских играх). Более половины заядлых игроков говорят о том, что именно возможность «живого» общения больше всего привлекает и удерживает их в игре;

– познавательность. Можно побродить, скажем, по Древнему Египту или поучаствовать в восстании Спартака.

Отрицательные стороны компьютерных игр

– вырабатывается привычка уходить от проблем в «виртуал», что негативно сказывается на умении решать свои проблемы вообще;

– отрицательно сказываются на физическом здоровье, так как игровой процесс построен в первую очередь на эмоциональности и сам по себе не требует от игрока физической активности. Особенно страдает зрение;

– отрицательно отражаются на нервной системе и психике, утомляемых постоянными перегрузками, вызванными многочасовым сидением за монитором. Игроманы стараются проводить максимум из

доступного времени за компьютером, часто жертвуя сном ради игры; большинство игроманов в жизни замкнутые, не общительные люди, отвыкшие (либо не научившиеся) общаться напрямую без помощи компьютера;

– после яркой, насыщенной событиями игры сложно переключатся на реальный мир, с его повседневными рутинными заботами.

– Мозговой штурм. Какие опасности я знаю в интернете? С чем я лично сталкивался (или боюсь столкнуться)? оскорбления, вирусы, мошенники, постоянное пребывание в сети, неадекватные люди, угрозы, преследования и т.д.

Ознакомление с презентацией «Безопасный Интернет» (15 минут) Педагог или сами студенты кратко комментируют каждый слайд.

5. Упражнения, направленные на развитие умений, необходимых для противостояния опасностям сети Интернет. Упражнение «Пирамида» (5 минут)

Инструкция. Преподаватель выбирает одного из класса; подросток выходит и приглашает к себе двух других. Те двое, в свою очередь, выбирают себе каждый по два участника. Таким образом, каждый «приглашенный» должен пригласить к себе еще по два человека. Игра заканчивается, когда не остается никого, кто еще сидит на своем месте.

– Обратите внимание на то, как мало времени потребовалось, чтобы поднять всех присутствующих со своих мест. На что похоже то, что мы сейчас делали? Есть ассоциации? Все началось с одного человека, а закончилось всей группой, - да, напоминает пирамиду. Как вы думаете, каким образом пирамида может быть связана с Интернетом? (люди регистрируются в соцсетях и приглашают других). Каждый решает сам, становится ли частью пирамиды или нет, но давление общества очень сильно, и в данный момент очень мало людей, которые имеют возможность пользоваться интернетом, не находятся под влиянием сетевого механизма.

6. Релаксация. Визуализация «Путешествие по Интернетлэнд»(5-7 минут)

– Упражнение необходимо начать с дыхательной подготовки.

– Предложите детям занять удобное положение, выпрямиться; объясните им, что с выпрямленными спинками легкие больше вдыхают кислорода, следовательно, мозг их лучше дышит.

– Закройте глаза, сделайте три медленных глубоких вдоха так тихо, чтобы никто их не слышал, и медленно выдохнуть (возможно музыкальное сопровождение для фона (тихо), музыка инструментальная, ассоциирующаяся с интернетом, компьютером и т.п.). Начните говорить тихим голосом:

«Сегодня мы совершим маленькое путешествие. Мы будем использовать нашу фантазию и, фантазируя, создавать различные картинки в нашем воображении. Мы с вами отправимся в удивительную страну Интернетлэнд. Мы все пользуемся Интернетом, заходя туда со своего компьютера или телефона, но ещё ни разу не путешествовали в эту страну в своих фантазиях. Вы дышите спокойно и представляете себе, что идете по необычной тропинке. Тропинка выстлана Лайками и Смайлами. День прекрасный, погода в Интернетлэнд хорошая, солнечная, вы огляделись вокруг - вас окружает сказочный мир Интернетлэнд. Что вы видите вокруг себя, осмотритесь внимательно и запомните все-всё, что вас окружает… (ПАУЗА – 10-12 секунд). Вы освоились и уже увереннее идёте дальше. Вы попали в какой-то просторный зал, огромный, бесконечный, с множеством разных дверей, больших и маленьких, очень красивых, привлекательных и манящих вас зайти. Вам очень хочется заглянуть за каждую дверь, но что-то подсказывает вам, что не во все двери можно входить. Тут вы внимательнее присмотрелись… на некоторых дверях видны надписи: Осторожно! Не входить! Как вы думаете, что за этими дверями… (ПАУЗА – 10-12 секунд). Найдите двери без предостерегающих надписей и зайдите в одну из них. Запомните, что вы там увидели? Почему вы вошли именно в

эту дверь, что вас привлекло? Запомните там всё как следует... (ПАУЗА – 10-12 секунд).

Вам пора уходить. Вы потихоньку перелетаете с помощью высокоскоростного Интернета из страны назад в эту комнату. Вы ощущаете ваше тело, как вы сидите на стуле и как ваши ноги дотрагиваются до пола. Вы начинаете слышать звуки в комнате. Когда вы почувствуете себя готовыми, спокойно открывайте глаза».

Вопросы:

- Ваши фантазии вы оставляете при себе, возможно сегодня вам приснится яркий красочный сон о путешествии.
- Желающие могут поделиться своими фантазиями.

7. Рефлексия занятия (5-6 минут). Нужно разработать правила поведения в сети Интернет, используя опорные слова.

Помни о

Позаботься о

Никогда не

Всегда

Думай о

Обрати внимание на

Постарайся

Посоветуйся с

Узнай о

Не забудь

Ни в коем случае не

Сделай

Занятие 2. «Моя сетевая безопасность. Кибер-буллинг. Будь в себе уверен» (55-60 минут)

Цель: Формирование и развитие навыков поведения в опасных ситуациях, связанных с сетью Интернет, навыков уверенного поведения

Задачи:

1. Формировать у подростков представления о кибер-буллинге.
2. Развивать навыки ответственности за свои поступки.
3. Формировать навыки конструктивного поведения в ситуациях, связанных с интернет-травлей.
4. Воспитывать умение аргументировать своё мнение.
5. Отрабатывать навыки уверенного поведения и саморегуляции.
6. Способствовать овладению психотехническими приемами, направленными на создание положительного образа "Я".

Материалы: цветные карандаши (фломастеры), классная доска (маркерная доска), символы правил поведения на занятий, листы для дополнительного изготовления символов по ходу занятия, скрепки по количеству обучающихся, конверт средних размеров, приклеенный к листу бумаги с надписью «Как правильно себя вести», листки бумаги (А5 – А6), листки для рефлексии, мяч.

Ход занятия

1. Приветствие

Упражнение «Внимание на меня!» (2 минуты). Всем участникам игры предлагается выполнить одну и ту же простую задачу. Любыми средствами, не прибегая к физическим действиям, нужно привлечь внимание окружающих. Задача усложняется тем, что одновременно ее выполняют все участники.

2. Правила поведения на занятии.(1 минута)

Повторяются правила, сформулированные на предыдущем занятии, добавляются новые, рисуются соответствующие символы.

3.Разминка

Упражнение «Скрепка» (5-7 минут). Каждому участнику дается металлическая скрепка. За 20 секунд студенты должны разогнуть и выпрямить ее как можно лучше, причем делать это нужно только руками. Разогнутые скрепки демонстрируются и, путем голосования выбирается из

них самая ровная. После скрепки возвращаются студентам; снова в течение 20 секунд им нужно придать прежнюю форму. Скрепки показываются группе, для сравнения к ним добавляется новая скрепка.

- Кто лучше всех сумел восстановить свою скрепку в первоначальном виде?
- Достигли ли вы желаемого результата?
- Похожа ли скрепка после восстановления на первоначальную?
- Как можно перенести это упражнение на человеческие отношения?

Вывод: восстановленная скрепка похожа на скрепку, ей даже можно пользоваться – но она не такая, как раньше; очень трудно, а порой невозможно восстановить в прежнем виде то, что изменилось. Некоторые последствия наших решений, нашего поведения нельзя устранить полностью. Так же и с людьми: любое действие изменяет как отношения между людьми (можно их навсегда испортить, можно восстановить – но прежними они уже не будут), так и может изменить личность самих участников. Изменения бывают опасными и необратимыми, поэтому в общении всегда следует выбирать ту линию поведения, которая позволит избежать серьезных последствий.

4.Информационный блок (15 минут)

Сегодня мы продолжаем тему безопасности в интернете и поговорим о таком феномене, как кибер-травля. Но прежде, чем мы начнем, предлагаю вам ответить «да» или «нет» на утверждения. Вы можете поднимать руки или просто подсчитывать про себя, сколько у вас положительных ответов.

Утверждения:

1) вы периодически сталкивались с интернет-троллями (с теми, кто оскорбляет, обижает, обзывает тебя в Интернете),
2) вы получали обидные комментарии к фотографиям или видеозаписям,

3) один раз или больше вы становились свидетелями оскорблений людей в сети интернет,
4) несколько раз вам писали оскорбительные сообщения незнакомые люди,
5) хоть раз вы получали письма с угрозами,
6) с вами выкладывали смешные видеоролики без вашего согласия,
7) вас без предупреждения и причин отправляли в бан-лист,
8) о вас распускали нелепые слухи,
9) вы пересылали знакомым конфиденциальные фотографии, которые позже обнаруживали в сети,
10) кто-либо создавал в интернете страницу с вашим именем (фейк),
11) вас оскорбляли в онлайн-играх.

Кто ответил положительно на 5 вопросов? Кто на все 11? У кого вообще нет положительных ответов?

– Ребята, каждый из вас побывал хотя бы раз в одной из ситуаций, и чувствовал себя крайне некомфортно. Подобные явления носят название кибербуллинга.

Многие люди, независимо от возраста, находясь в виртуальном пространстве могут стать жертвами буллинга, или травли, - систематически повторяющихся агрессивных выпадов в их сторону. *(сетевой буллинг показан в фильме «Кибер-террор», «Запрос в друзья», «Убрать из друзей).* Буллинг происходит от английского «бык» со сводными значениями агрессивного нападения, задирания, придирок, провокаций. Кибербуллинг - это нападение с целью причинения психологического ущерба. Касается каждого человека, который пользуется интернетом, особенно социальными сетями. Чем больше соцсетей захватывает человек, тем более он становится уязвимым.

Булли обращаются к жертве по следующим каналам:

– Телефон: звонки, сообщения, съемка видео.

– Чат: угрозы, оскорбления, игнорирование, ввод в доверительные отношения.
– Е-мейл: рассылка злобных сообщений, непристойных и вредоносных материалов, взлом почты.
– Соцсети: обидные комментарии, распространение непристойностей, взлом и размещение в аккаунте неприятной информации, создание группы ненависти, фейка страницы.
– Видеопорталы: непристойные и позорящие видео.
– Игры: оскорбления, уничтожение героя, изоляция от участия в игре.

Мозговой штурм

Как вы думаете, почему людям хочется этим заниматься? Зачем травить других? (*скука, зависть, месть, неприязнь, борьба за власть, самоутверждение превосходство, центр внимания, комплекс неполноценности, личностный кризис).*

Целью буллинга является сокрытие агрессором своей неполноценности за маской жестокости.

Какие особенности могут подтолкнуть человека к занятию интернет-травлей?

– Низкий уровень воспитания;
– Неадекватная заниженная самооценка;
– Внутриличностная агрессивность, зависящая от индивидуальных особенностей;
– Желание сохранить статус в группе и соответствовать группе;
– Желание доминировать над другими;
– Семейное насилие;
– Внутрисемейные конфликты;
– Высокая конфликтность;
– Низкая устойчивость к стрессу.

Буллеры – это:

- Активные, общительные подростки, претендующие на роль лидера;
- Агрессивные подростки, использующие для самоутверждения безответную жертву;
- Подростки, стремящиеся быть в центре внимания;
- Подростки высокомерные, делящие всех на «своих» и «чужих» (что является результатом соответствующего семейного воспитания);
- Максималисты, не желающие идти на компромиссы;
- Подростки со слабым самоконтролем, которые не научились брать на себя ответственность за свое поведение;
- Подростки, не обученные другим, лучшим способам поведения, т.е. не воспитанные.

Ребята, особенности зачинщика травли мы с вами обсудили. А какими особенностями может обладать человек - жертва сетевой травли? *(Жертвой кибербуллинга может стать каждый человек, и ребенок, и взрослый, независимо от сферы деятельности, состояния здоровья, особенностей внешности)*. Любой человек может стать виновником забавной ситуации, превратившейся в популярный ролик в интернете; каждый может попасть в эпицентр вихря насмешек и грубых комментариев…

Естественно, ни одному человеку не будет приятно, когда его оскорбляют. Большинство из вас призналось, что были случаи получения бесцеремонных сообщений, критики в сети; *какие чувства вы испытывали?* (ответы детей).

Точно то же самое чувствует жертва травли.

5. Упражнения, направленные на развитие умений, необходимых для противостояния опасностям сети Интернет

Упражнение «Конверт с предложениями» (7 минут). Инструкция: сейчас вы можете написать на листочке предложения о том, как правильно вести себя в сети Интернет. Подумайте, вспомните то, о чем мы с вами

говорили, и напишите свои соображения, как повести себя, чтобы не стать жертвой травли в интернете, либо как себя вести жертве.

Листочки с предложениями из конверта размещаются на доске. Рекомендации по безопасному поведению в сети (подсказка):

1) сами в интернет-пространство негатив не выплескивайте. Откажитесь от комментариев по поводу чужих особенностей и увлечений, неизвестно, какое воздействие они окажут на человека. А за мат вы можете понести наказание.

2) Интернет – место неконфиденциальное, обидчиков всегда можно найти. Это тоже следует помнить, когда вас оскорбляют и когда оскорбляете вы. И все, что вы отправляете, удалить из интернета может оказаться невозможным.

3) храните доказательства фактов нападений. Если вы решите дать делу ход, то вы будете иметь возможность распечатать и показать действия булля родителям, друзьям или полиции. Появляется услуга нотариально заверенного скриншота.

4) редко повторяющиеся выпады нужно игнорировать. Или же забанить недруга. В крайнем случае, смените электронные контакты и социальные сети.

5) при наличии в сообщениях угроз и порнографических материалов лучше обратитесь в правоохранительные органы.

6) видите в интернете буллинг? Лучше не ввязываться. Но можно сделать это крайне вежливо. Откажитесь от виктимблейминга – обвинения жертвы. Люди, оказавшиеся в неприятной или смешной ситуации, не заслуживают травли и публичного унижения. Лучше, если вы в таком случае обозначите свою позицию против булля; поддержите жертву и сообщите (взрослым, администрации сайта, на горячую линию) о нарушении человеческих прав.

7) И другое…

Мозговой штурм (7 минут)

Что такое уверенность в себе? Что включает понятие уверенного поведения? Как можно охарактеризовать уверенного в себе человека? (ответы детей)

Уверенный в себе человек знает, что он имеет определенные права, умеет точно определить и выразить свои желания, потребности и чувства так, чтобы это не затронуло окружающих. Он умеет строить отношения с другими людьми, что называется "на равных", вне зависимости от положения, которое те занимают, уважает позиции и статус других людей.

6.Релаксация (под музыку).

Упражнение «Круг уверенности» (7 минут)

Инструкция: Представьте невидимый круг диаметром 60 сантиметров на полу примерно в полуметре от себя. Зайдите в этот круг и вспомните прекрасное время, когда вы были на «волне успеха». В этой ситуации максимально проявились все ваши способности. Всё было хорошо, удача сопутствовала вам. Отметьте для себя и запомните то, как вы видите, слышите и чувствуете окружающий мир в ситуации успеха. Как обычно уверенно звучит ваш голос, как устойчива и горда осанка. Представьте себя в наилучшем состоянии.

Вернитесь из круга в нейтральное состояние. Запомните комплекс в «Круге уверенности». Этот комплекс станет ключом к уверенности и спокойствию, когда они вам будут необходимы. Когда возникнет особая ситуация, требующая уверенности, войдите в своих мыслях в этот круг.

7.Рефлексия (10 минут)

Упражнение на завершение «Без смайлов». В Интернет-пространстве все выражают свои эмоции при помощи улыбающихся или грустящих кружков – смайлов. Ребятам предлагается определить свое эмоциональное состояние и нарисовать его на листке, не изображая известные смайлы. После рисования каждый показывает группе свой рисунок – все стараются угадать, что изображено, - и говорит, что он испытывает в данный момент, после чего проговаривает свои пожелания группе.

Упражнение на завершение «Чуточку сильнее». Ребята передают друг другу мяч. Пусть каждый участник начнет фразу, которая будет отражать, какие знания были получены, и заканчиваться следующим образом: «.. и поэтому сегодня я стал (-а) чуточку сильнее».

Занятие 3. «Интернет-преступники. Правила безопасного поведения в Интернете» (80-90 минут)

Цель: Формирование и развитие навыков поведения в опасных ситуациях, связанных с Интернет-мошенничеством, Интернет-преступлениями.

Задачи:

1. Познакомить с видами Интернет-преступлений, в частности Интернет-мошенничества.
2. Формировать навыки эффективного поведения в ситуации мошенничества.
3. Развивать навыки достойного отказа.
4. Способствовать снятию психоэмоционального напряжения, вызванного использованием сетью Интернет.
5. Актуализировать у детей и подростков полученных знаний.
6. Развивать навыки поведения в опасных ситуациях.

Материалы: карточки с ситуациями, картинки с изображением чемодана, корзины, мясорубки, таблички с названиями опасностей в Интернете, скриншоты страниц с опасными предложениями

Ход занятия

1. *Приветствие, психологический настрой* (3 минуты)

Поприветствуем друг друга разными способами по условному сигналу: хлопком ладонь к ладони, плечом и т.д.

Упражнение-энергизатор «Компьютер». Студенты делятся на 3 группы: «монитор», «процессор», «клавиатура». Когда преподаватель говорит какое-либо из названий, участники группы меняются местами.

Когда преподаватель говорит «компьютер» - меняются местами все участники занятия.

2. Правила поведения на занятии (1 минута). Напоминаются правила работы в группе, при необходимости добавляются новые, которые подходят для данного занятия (добавляем символы).

3. Разминка (15 минут)

Упражнение «Что делать». Подросткам раздаются карточки с описанием спорных ситуаций, которые могут произойти в виртуальном пространстве (по 1 на группу). После обсуждения подростки зачитывают свою ситуацию и отвечают на вопросы.

- *какую угрозу несет данная ситуация?*
- *что бы вы предложили делать в данной ситуации?*

1. К вам на почту поступает письмо с просьбой о материальной помощи, т.к. автор письма студент/начинающий/в сложной ситуации/денег нет, кушать нечего. На вас никто не давит, желаемая сумма может не указываться. Помочь человеку или нет – только ваше дело.

2. Вам приходит письмо о крупном выигрыше: вы выиграли деньги/машину/что-то еще, приз будет выслан/счет активирован, как только вы переведете некоторую сумму (пошлина, транспортные расходы и тд.).

3. Вы заходите на сайт, на котором вы уже зарегистрированы, по ссылке, но вам надо заново вводить почту и пароль от нее.

4. Вам приходит письмо с уведомлением, что аккаунт на каком-либо сайте взломан, или может быть заблокирован или удален (и т.д.), чтобы этого не случилось, необходима оплата (даже когда вы даже не регистрировались на сайте).

5. Вам приходит сообщение насчет «нелегального доступа к услугам сайта», спама с вашей страницы, появляются угрозы выложить в сеть какие-либо Ваши материалы, где главным условием избавления от

проблемы являются ваши действия по отправлению денежных средств шантажисту.

6. Вас приглашают в группу, предлагают принять участие в интересной игре-квесте, где нужно выполнять интереснейшие задания и размещать фотоотчёт в соцсетях.

Как вы думаете, о чём сейчас пойдёт речь?

4. Информационный блок (15 минут)

Ребята, как вы уже поняли из предыдущего упражнения, нашей темой занятия станет мошенничество в интернете. Интернет-пространство расширяется, и с этим связано развитие кибер-мошенничества. Если люди уже научились распознавать мошенников в реальной жизни, и уже не «ведутся» на обычные шутки, то мошенников в интернете распознать гораздо сложнее. *Как вы считаете, по каким причинам?*

Да, глазами преступников не увидишь, и понять, что и как они могут сделать, непросто.

В кибер-пространстве мошенники работают по нескольким направлениям.

1. Денежные «мышеловки»

1) «узнай местоположение по номеру телефона»

Вам предлагается зарегистрировать программу распознавания либо бесплатно, либо со взносом определенной суммы; программа часто оказывается обыкновенным вирусом. В любом случае, человек что-то теряет – деньги со своего счета или же информацию со своих аккаунтов, связанных с компьютером или телефоном. Либо незадачливого «шпиона» начинают терроризировать звонками и электронными письмами.

Как поступить. Правоохранители предупреждают, что узнать местоположение можно только с согласия абонента, либо по запросу в полиции (от оператора). Иные варианты не действуют. Поэтому откажитесь от слежки, не отправляйте смс и сообщения на указанные номера и уважайте приватность своих ближних.

2) «беспроцентный кредит»

Пользователю, желающему взять кредит, предлагают предоставить его быстро, легко и в любом объеме, если на счет мошенников будет перечислена круглая сумма. Действия преступников строятся как зеркальное отражение закона: к людям выезжают сотрудники, заполняются необходимые документы (получается согласие в том, что все добровольно и без претензий). Итог – ни денег, ни кредита. Как поступить. Кредиты лучше не брать вообще; при необходимости сделайте заем у кого-нибудь из друзей или знакомых. При отсутствии возможности возьмите кредит в известном банке, придя лично в его филиал.

3) «магазин на диване»

Вам предлагается приобрести желаемый товар по привлекательной цене (раз в 5 ниже среднестатистической), а возможно и вовсе бесплатно – вроде конфискат, вам делают подарок. Или к вам попадает журнал с товарами от известного магазина. Есть предложение – получить за заказ на ЭН-ную сумму ценный приз.

4) «увеличение дохода»

Вы получаете письмо, где указывается, что денежный сайт предлагает эффективный способ удвоения капитала, (отправь 100 р, получи 500). Или вам приходит сообщение о смерти дальнего родственника, наследником которого являетесь вы, однако нужно переслать налог на наследство. Как поступить. Ни в коем случае ничего не высылайте; проверьте, действительно ли у вас был четвероюродный внучатый дядя из Канады, и ждите адвоката. Все юридические вопросы решаются с глазу на глаз, а не в интернете.

5) «лотерея»

Вам приходит письмо о крупном выигрыше: вы выиграли деньги/машину/что-то еще, приз будет выслан/счет активирован, как только вы переведете некоторую сумму (пошлина, транспортные расходы и тд.). Вы не участвовали в конкурсе – неважно. Даже не слышали о нем –

тем более. Это очень интересно, просыпается азарт – получить нечто, при этом ничего не делая.

Как поступить. Вспомните, принимали ли вы участие, знаете ли организацию, откуда у нее ваши контакты; не знаете ответа на вопрос – забудьте о сообщении и ничего не переводите.

6) отправка смс

Ситуация первая. «Ваш аккаунт блокирован, подтвердите смс… вы выиграли, отправьте смс… помоги выиграть в голосовании…, получи доступ к сайту…» Стоимость СМС - в 5-10 раз больше обычной.

2. «попрошайничество»

1) помощь в трудной жизненной ситуации

Ситуация первая: к вам на почту поступает письмо с просьбой о материальной помощи, т.к. автор письма студент/начинающий/в сложной ситуации/денег нет, кушать нечего. На вас никто не давит, желаемая сумма может не указываться. Помочь человеку или нет – только ваше дело.

Ситуация вторая: вам приходит письмо с официального сайта благотворительной организации (детдома, приюта) с просьбой о материальной помощи какой-либо категории людей/человеку в социально опасном/затруднительном положении.

Как поступить. При желании помочь – проверьте адрес сайта (не дублер ли это), на кого оформлены реквизиты для перечисления денег. Позвоните в организацию (посетите ее), уточните номер счета и достоверность размещенной информации.

3. «техподдержка»

Ситуация первая: вам приходит письмо с уведомлением, что аккаунт на каком-либо сайте взломан, или может быть заблокирован или удален (и т.д.), чтобы этого не случилось, необходима оплата (даже когда вы даже не регистрировались на сайте).

Как поступить: не оплачивать, не переходить по ссылкам (можете подхватить вирус) и не вводить данные. Зайдите на сайт с проверенного

адреса, обновите страницу, можете обратиться к администратору сайта с вопросом.

Если все же успели ввести пароль, сразу же смените его.

4. шантаж

В эту категорию относятся все сообщения насчет «нелегального доступа к услугам сайта», спама с вашей страницы, угроз выложить в сеть какие-либо материалы, где главным условием избавления от проблемы являются ваши действия по отправлению денежных средств шантажисту.

Как поступить. Можете написать провайдеру о спаме с угрозами, либо в техподдержку сайта, услугами которого вы якобы пользуетесь. Любую угрозу можно заскринить, распечатать и обратиться в полицию.

5. механический ущерб

1) вирусы

«Вы реальный человек – введите свой номер телефона». Вам либо приходит смс для ответа, либо вы автоматически подписываетесь на какую-то телефонную услугу и у вас со счета списывается ежедневно пара десятков рублей. Если вы получили сообщение со ссылкой на скачивание открытки, музыки, картинки или какой-нибудь программы, не спешите открывать её. Перейдя по ссылке, вы можете, сами того не подозревая, получить на телефон вирус или оформить подписку на платные услуги.

Как поступить. Внимательно читать всю информацию, особенно мелким шрифтом, со страниц, в частности - внизу сайта. Если не помогло, немедленно обратитесь в салон связи отключать услугу. Посмотрите, с какого номера было отправлено вам сообщение. Даже если сообщение прислал кто-то из знакомых вам людей, убедитесь в этом, позвонив оппоненту. Если отправитель вам не знаком, не открывайте письмо.

Помните, что установка антивирусного программного обеспечения на компьютер или мобильное устройство повышает вашу безопасность.

2) сайты-фейки

Вы заходите на сайт, на котором вы уже зарегистрированы, по ссылке, но вам надо заново вводить почту и пароль от нее. Как поступить. Проверьте адрес сайта и перейдите по проверенной ссылке.

6. работа в интернете

Интернет является одним из способов заработка, но человек может стать жертвой мошенников: когда он выполнит работу по переводу текста или написанию реферата, то может остаться без обещанной платы. Как поступить. Собираясь работать в сети, помните, что главный принцип – сначала оплата (хотя бы половинная), потом – работа.

Обсуждение: сталкивались ли вы с каким-то видом мошенничества в интернете?

5. Упражнения, направленные на развитие умений, необходимых для противостояния опасностям сети Интернет

Ребята, помимо мошенничества, в социальных сетях, как вы знаете, процветают деструктивные сайты и группы, которые склоняют, вынуждают играть в их игры, если отказываешься - угрожают, шантажируют. Вспомним тему кибербуллинга на предыдущем занятии. Будем учиться давать отпор Интернет-преступникам, Интернет-мошенникам, шантажистам и т.д.

Упражнение «Привлекательное предложение» (10-12 минут)

Подростки разделяются на пары. Один человек должен предложить другому что-либо привлекательное для него (в деталях) (в том числе и участие в квест-игре), оппонент придумывает аргументы, почему ему это не нужно, и он от этого откажется. После ребята в паре меняются.

Обсуждение: легко ли было тебе отказаться от предложения? Какие методы убеждения использовал предлагающий?

Большая ролевая игра «Опасности сети Интернет» (15 минут).

Студентам раздаются роли (таблички с названиями опасностей в Интернете). На внешней стороне таблички написана приемлемая роль (например СМС, электронное письмо, Друг, Реклама, Интересный сайт,

Антивирус, но с обратной стороны (невидимой для окружающих) на многих из них написана истинная роль, которую нужно будет грамотно сыграть: вирусы, спам, вредоносные ПО (программное обеспечение), Интернет-хам (тролль), поддельный сайт, Интернет-мошенник (попрошайка), Незнакомец, который хочет заманить куда-нибудь, вызвать на встречу и другие. Несколько ребят играют роль пользователей, которые должны взаимодействовать с остальными (носителями пользы и вреда в Интернет-пространстве) и грамотно принимать или отсеивать поступающую информацию.

Рефлексия упражнения:

– Что вы поняли, проиграв это упражнении?

– Трудно ли было распознать истинные мотивы оппонента (того, с кем вступаете в контакт, общаетесь)?

– Трудно ли было играть две роди одновременно (явную и скрытую)?

– Какие выводы сделаем?

Ребята, учтите, что в этой игре вы имели возможность видеть глаза оппонента, жесты, движения и т.д., а при общении через Интернет, как мы уже говорили, мы не видим оппонента и не можем определить, хороший это человек (программы, предложения, которые он предлагает) или плохой.

6.Релаксация. Представьте, что Вы долго работали за компьютером. Устали, Вам нужно восстановиться. Разомнём шею (круговые движения), плечи, выпрямить спину.

Упражнение «Снеговик» (2 минуты)

Представьте снежный морозный день. Подростки слепили снеговика. Он стоит такой весь замёрзший. Голова замёрзшая (напряжена), плечи, руки, туловище, ноги. Пригрело солнышко, сильно пригрело. Снеговик стал таять (постепенно расслабляем названные части тела): растаяла

голова, шея, плечи руки, туловище, ноги – растаял весь снеговик, превратился в лужу.

7.Рефлексия занятия. Сегодня у нас с вами последнее занятие, и нужно будет вспомнить правила безопасного поведения в интернете. Вопрос: кто помнит какие-либо правила из предыдущих занятий? Упражнение «Мое видение правил поведения в Интернете» (7 минут)

Каждому участнику в кругу предлагается назвать одно правило безопасного поведения в Интернет пространстве. Правила не должны повторяться.

(Подсказка) Правила безопасного поведения и общения в интернете.

1) законодательно в сети запрещены определенные действия со стороны вас как пользователя. Некоторые из них еще и аморальны:

- передача по сети информации, оскорбляющей честь и достоинство человека (в т.ч. призывы к насилию, разжигание межнациональной розни, порнографические материалы),

- разработка и распространение вредоносных программ, занятия хакерством.

2) когда вы ведете беседы, помните, что общаетесь не с ботом, а с реальным человеком, который может испытывать эмоции, чувства. Человека обидеть легко, а исправить ситуацию сложно. Поэтому старайтесь соблюдать те же правила общения, что и в «реале» (будьте вежливы, тактичны, не оскорбляйте собеседника и др.) и придерживайтесь рамок закона.

3) не навязывайтесь. Уважайте не только свое время, но и чужое. При отказе собеседника от разговора переключитесь на что-либо другое и не досаждайте ему. Помните, что нет – значит нет. Не требуйте мгновенного ответа на сообщение.

4) по возможности, старайтесь отвечать на сообщения быстро. Если с вами нацелены пообщаться, а у вас нет времени для полноценного разговора, предупредите об этом собеседника.

5) если вас просят о помощи информационного характера, не стоит упрекать оппонента в невежестве и насмехаться над ним. Если вам известен ответ на вопрос собеседника, или вы знаете, где этот ответ можно найти, напишите ему об этом.

6) избегайте конфликтов и сами их не провоцируйте. Если собеседник не принимает вашу точку зрения, помните, что это – его право. Вместо того, чтобы ругать его и доказывать свою правоту, предоставьте ему возможность ознакомиться с фактами по интересующей его тематике. Если собеседник перешел на личности и оскорбляет вас, предельно вежливо завершите разговор.

7) не выкладывайте информацию личного характера в сеть: адреса, телефоны, имена электронных почтовых ящиков. Помните, что злоумышленники могут воспользоваться этой информацией в личных целях.

7.1) это относится и к любой информации о вашем собеседнике – не разглашайте ее. Не выкладывайте в открытый доступ сообщения из конфиденциальных (рабочих, дружеских, романтических) разговоров, не получив согласие собеседников, это нарушение права на частную переписку; такое поведение выявляет сплетников и аморальных людей.

8) не выкладывайте в сеть и не отправляйте другим лицам фото и видео (особенно интимного содержания) – ни свои, ни друзей. В том числе, не отправляйте друзьям: при взломе почты (странички) материалы могут либо попасть на всеобщее обозрение, либо ситуация может повлечь за собой шантаж.

9) вступая в переписку или комментирование любого материала на разных сайтах, имейте в виду, что анонимность в интернете – иллюзорна, и узнать об обладателе определенной странички или ника несложно. Будьте корректны в своих действиях, чтобы не нанести вред другим пользователям и своей онлайн-репутации.

10) если вы испытываете негативные эмоции и ваше состояние требует эмоциональной разрядки, писать в интернет гневные сообщения, посты и комментарии – плохой выход. Состояние изменится через малый промежуток времени, а историю ваших действий интернет (возможно и пользователи) будет хранить гораздо дольше. Постарайтесь успокоиться, подумайте, потом уже вступайте в беседы.

11) игнорируй единичные сообщения оскорбительного характера (прим.: оскорбления – часто начальная стадия интернет-травли), поскольку «игнор» является эффективным способом предотвращения дальнейших неадекватных действий оппонента. Целью сообщений является нарушение эмоционального равновесия человека. Если агрессор не прекращает свои выпады, то наилучшим выходом будет его блокировка («черный список» во вконтакте и мэйл.ру, «блокировка» в фейсбук, «заблокировать пользователя» в инстаграм).

11.1) если не желаете получать комментарии и сообщения от различных пользователей – настройки приватности вам в помощь.

12) при обнаружении оскорбительной информации, размещенной на сайте, целесообразно обратиться к администратору сайта с просьбой удалить контент.

13) при наличии угроз или непристойных (порнографических) сюжетов в сообщениях игнорировать их не следует. Скопируйте (заскриньте) неприятные письма, распечатайте страницы и со всеми доказательствами смело идите в правоохранительные органы.

13.1) подтверждения фактов неадекватных обращений следует оставить и хранить в сети столько, сколько потребуется правоохранителям.

14) случайно став очевидцем сетевой травли, воздержитесь от обвинения жертвы (виктимблейминга), поскольку это не просто некультурно и аморально, но и может нанести вред как жертве, так и вам в случае перехода дела в правоохранительные органы. Если вы решите включиться в беседу, занимайте сторону жертвы, а не агрессора:

попытайтесь предоставить жертве эмоциональную поддержку, выступайте против негативных действий агрессора, сообщите взрослым (правоохранителям) о факте буллинга в интернете.

14.1) наиболее целесообразно обращаться сразу в прокуратуру, чтобы ход дела развивался быстрее.

15) доверяйте, но проверяйте. В интернете много мошенников, ими могут оказаться самые милые люди, желающие с вами познакомиться.

15.1) если человек решил завести с вами романтические отношения, настаивайте на личной встрече в любом случае. Есть деньги на оплату интернета – и на дорогу к объекту романтики найдутся. Старайтесь назначить встречу днем и в людном месте, если человек отказывается от такого варианта, то отложите встречу, перенесите ее на более удобный день. С теми же условиями.

15.2) если человек пишет, что отправил вам подарок, удостоверьтесь в том, что доставка оплачена. Иначе есть большая вероятность, что у вас не окажется ни подарка, ни определенной суммы денег.

15.3) когда к вам обращаются с просьбой о материальной помощи в связи с чем-либо и у вас появляется желание помочь, попросите оппонента предоставить подтверждения того, что он находится в сложной ситуации.

15.4) при появлении сообщения от близкого человека о том, что ему срочно нужны деньги и номером счета (телефона), позвоните ему на действительный номер и уточните, действительно ли требуется помощь. Вообще, хорошо иметь телефонные номера всех своих онлайн-друзей на всякий случай.

15.5) при решении работать фрилансером, если вы попадаете на сайт с работой, где требуется внести сумму денег, чтобы зарегистрироваться, не переводите деньги и найдите другой сайт.

15.6) предоплата – обязательное условие работы в интернете. Если вам не заплатили за статью – не высылайте ее.

15.7) при решении работать веб-моделью помните о том, что если в контракте нет услуг интимного характера, вы их не предоставляете и имеете право прекратить работу и обратиться в правоохранительные органы.

15.8) прежде, чем связывать себя с сайтом работы, проверьте в интернете отзывы о сайте и компании, осуществляющей деятельность.

16) избегайте скачивать материал с непроверенных сайтов, особенно если там требуется ввести свои данные и пароль от почты, это может привести к заражению компьютера. Прежде, чем сохранить материал на свой компьютер, убедитесь, что файл имеет правильное разрешение.

17) не переходите по ссылкам в социальных сетях, вы можете быть перенаправлены на мошеннический сайт-обманку.

Обсуждение: какие приобретенные знания оказались новыми для меня (были ли уже случаи, когда они мне пригодились?)

Упражнение «Чемодан. Корзина. Мясорубка» (10 минут)

Участники выбирают картинки чемодана, мусорной корзины или мясорубки в зависимости от полезности полученных знаний и отработанных навыков по теме безопасности в сети Интернет (или располагаются по принципу «Четыре (три) угла» в соответствии с размещёнными там картинками чемодана, корзины и мясорубки.

Чемодан – знания, умения и навыки были полезными, я возьму их с собой и буду пользоваться.

Мусорная корзина – ничего для меня не было полезным, мне не пригодятся эти навыки.

Мясорубка – мне ещё нужно осознать то, что я узнал на занятиях, обсудить с кем-то.

Ребята, наше занятие подошло к концу. Будьте внимательны и соблюдайте правила безопасности в интернете.

Приложение 5

АНКЕТНЫЙ ОПРОС

Спам, мошенники, вирусы... Все это каждый из нас слышал и, возможно, сталкивался. Просторы всемирной паутины не всегда безопасны. Но знаешь ли ты, какой этикет в сети Интернета? Что безопасно, а что несет опасность? Тест на безопасность в интернете поможет тебе понять насколько ты защищен на его просторах. Опрос анонимный, но выберите, пожалуйста, свою группу

1) Письмо, которое пришло на твой почтовый ящик, содержит ссылку или файл. Как ты с ним поступишь?

а) Если адресант известен, то перед переходом по ссылке нужно прочитать название сайта, на который она ведет, а файл – проверить антивирусом.

б) Ссылки и файлы в письмах, которые не попали в папку "Спам" - безопасны.

2) К тебе в контакт-лист (в социальной сети, мессенджере и т. п.) попросился кто-то, кого ты не знаешь. Что ты сделаешь?

а) Людей, которых ты лично не знаешь, заносить в списки друзей не желательно!

б) Только людей с фотографиями, даже не знакомых, можно добавить без страха в друзья!

в) Чем больше друзей, тем лучше! Можно добавлять абсолютно всех, даже без фото!

3) Как ты назовешься при регистрации на форуме?

а) Выберу ник, который совершенно не определяет мой возраст, пол и половую принадлежность.

б) Конечно же реальным именем и фамилией!

в) Подберу ник по типу "Елена85". Так многие делают!

4) Знакомый вызвался помочь тебе разобраться с почтовой программой и просит тебя назвать пароль от почтового ящика, чтобы установить необходимые настройки. Что ты сделаешь?

а) Свои пароли нельзя выдавать никогда и никому, о чем бы ни шла речь!

б) От почты пароль могу дать. Я там ничего не скрываю!

в) Конечно назову, он же помочь мне хочет!

5) Ты долго общаешься с человеком из форума, и он предлагает тебе встретиться. Какое место для личного знакомства ты предпочтешь: парк, кино или кафе?

а) Никакое! Интернет-друзья могут оказаться совсем не теми, за кого себя выдают, поэтому переносить встречи с ними в реальность не рекомендуется!

б) Кино, парк или кафе... Главное, что есть люди вокруг!

в) Куда назначит встречу - туда и пойду! Я ж давно общаюсь на форуме с этим человеком!

6) Один или несколько онлайн-собеседников критикуют тебя, часто переходят на оскорбления, всячески переиначивают и высмеивают твои слова. После общения с ними надолго остается неприятный осадок. Что ты предпримешь?

а) Любое общение, которое приносит негативные эмоции, нужно сразу прекращать без объяснений и оправданий, а агрессивных собеседников – заносить в черный список (исключать из друзей, блокировать, удалять из контактов и т. д.).

б) Попытаюсь наладить общение, стараясь оправдаться или объяснить ситуацию, чтоб меня верно поняли.

в) Если они в списке моих друзей - то придется смириться... Может им надоест устраивать кибербулинг надо мной?!

7) Многие из твоих собеседников, даже те, кого ты знаешь лично как воспитанных и культурных, позволяют себе в интернете другой стиль общения, допускающий нападки, ругательства, употребление

ненормативной лексики и т. п. Тебе это неприятно или ты, напротив, готов их поддержать и считаешь, что в сети можно вести себя более свободно и раскованно?

а) На просторах интернета необходимо вести себя абсолютно так же, как в жизни: никому не грубить, не сквернословить, оставаться вежливым и доброжелательным по отношению к другим пользователям.

б) Нормы поведения в виртуальном мире могут отличаться от принятых в реальности. И это нормально! Каждый выражает себя, как хочет!

в) Иногда можно позволить себе нагрубить, напасть, затролить... Это ж сеть интернета! Главное потом извиниться.

8) При общении в интернете кто-то просит твой номер телефона. Ты дашь его? И если да, то кому?

а) Номер телефона – такая же сугубо личная информация, как ФИО и паспортные данные, и раздавать его направо и налево очень опасно по многим причинам.

б) Это ж не паспортные данные... Конечно дам свой номер телефона. Но только тем, кто добавится ко мне в друзья!

в) Чем больше людей знают мой номер телефона - тем больше круг общения и связей!

9) Один из твоих виртуальных знакомых обещает тебе некую выгоду (покупку престижного гаджета с огромной скидкой, крупный выигрыш и т. п.), но для этого просит выведать информацию с банковских карт родителей или с их паспортов. Воспользуешься ли ты его предложением?

а) Конечно же нет! Это явно мошенничество. Любые аспекты, связанные с финансами, обсуждать в сети - табу!

б) Если у человека будет фотография на его странице, то значит он реальный и ему можно доверять. Попробую выгодно приобрести что-то новенькое!

в) Если скидка будет хорошая, то почему бы не воспользоваться таким шансом