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 умений по защите персональных данных в сети Интернет у студентов колледжа при преподавании специальных дисциплин

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:
74,47 % авторского текста

Работа рекомендована к защите
«20» 01 2024 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Деенков Андрей Николаевич

Научный руководитель:
д.тех.н., профессор
Дмитриев Михаил Сергеевич

Челябинск
2024

Содержание

ВВЕДЕНИЕ

Актуальность. Конституция Российской Федерации предоставляет право каждому свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ст. 29 ч. 4). Эти конституционные установления в полной мере относятся к любой информации, независимо от места и способа ее производства, передачи и распространения, включая сведения, размещаемые в информационно-телекоммуникационной сети Интернет [5].

В последние десятилетия число пользователей сети Интернет увеличилось многократно. Большая часть жителей планеты так или иначе используют «мировую паутину», оставляя в ней свои персональные данные, в том числе при регистрации на тех или иных ресурса сети. В современной Российской Федерации проблема защиты персональных данных в сети «Интернет» последние несколько лет является достаточно актуальной. Такая ситуация объясняется тем, что различными социальными сетями, мессенджерами, электронной почтой, да и просто самим интернетом пользуется большое количество граждан. При активном пользовании всем вышесказанным человек оставляет некоторые данные, которые могут дать информацию о нем. Эти данные могут быть различными, начиная просто от имени и фамилии и заканчивая всеми данными паспорта [5, с. 47-49]. Нередко случаются ситуации, когда в силу разных причин персональные данные того или иного гражданина становятся общедоступными, происходит так называемая утечка персональных данных человека.

Современная система образования, отражая потребности информационного общества, трансформирует парадигму обучения, переходя от традиционного образования в условиях ограниченного доступа к информационным ресурсам к образовательной деятельности в условиях всеобщей доступности информации.

Очевидной реальностью становится возрастание технологической, экономической доступности глобальных информационных сетей с размещёнными ресурсами, в том числе для обучающихся.

Фундаментальный рост и развитие различных видов массовой информации, информационных и коммуникационных технологий, глобальной сети Интернет и информационного общества оказывают самое прямое воздействие на интеллектуальное, психическое и физическое развитие подрастающего поколения, на формирование нравственного облика личности обучающегося.

В системе российского педагогического образования важнейшими задачами объективно становятся удовлетворение потребностей общества в создании надежных научно-педагогических, правовых, методических и организационных механизмов для обеспечения информационной безопасности субъектов образовательного процесса.

Для решения в системе среднего профессионального образования педагогических проблем, связанных с обучением основам информационной безопасности и защиты персональных данных как инвариантной составляющей информационной подготовки, направленной на формирование умений по защите персональных данных в сети Интернет, требуется системный подход, реализующий методологические, организационные, содержательные, дидактические аспекты. Система подготовки в области информационной безопасности и защиты персональных данных в сети Интернет должна быть детерминирована по всем уровням образовательной деятельности, как общего, так и профессионального образования: среднего, высшего, послевузовского, дополнительного, и ориентирована на различные специальности и специализации.

Становление научного направления «информационная безопасность и защита информации» в РФ связано с именами таких отечественных ученых, как А.А. Грушко, В.Ю. Гайкович, В.А. Герасименко, В.И.

Герасимов, Н.Н. Дмитриевский, Г.В. Емельянов, В.А. Минаев, А.П. Першин, А.А. Стрельцов и др. Правовые аспекты информационной безопасности нашли отражение в трудах Ю.М. Батурина, И.Л. Бачило, В.А. Копылова и др. Развитию теории и практики образования в области информационной безопасности посвящены исследования таких учёных, как Е.Б. Белов, К.К. Колин, А.Б. Кравченко, В.В. Мельников, Б.А. Погорелов, В.И. Ярочкин и др. Однако, анализ состояния проблемы информационной безопасности как проблемы педагогической позволяет сделать вывод о её недостаточной разработанности, поскольку различные её аспекты находят пока отражение большей частью в политологии, социологии, естественнонаучной, технической, правовой областях.

Существующая система образования в области информационной безопасности ориентирована, прежде всего, на подготовку специалистов, чья профессиональная деятельность напрямую связана с обеспечением информационной безопасности и защиты информации. К такого рода специалистам, относятся специалисты в области информационной безопасности и защиты информации: криптологи, аналитики по компьютерной безопасности, разработчики средств и систем безопасности, сотрудники органов, организаций и подразделений, занимающихся информационной безопасностью и защитой информации.

Для всех остальных категорий специалистов, подготавливаемых в системе среднего профессионального образования, имеющих доступ к информационным системам и использующих информационные и коммуникационные технологии в профессиональной деятельности, система обучения основам информационной безопасности в настоящее время только складывается, что усложняет решение задач обеспечения информационной безопасности, требующих ответственности и компетентности от каждого пользователя средств информационных и коммуникационных технологий.

Для педагогического сопровождения проблематики информационной безопасности в сфере образования необходима разработка электронного образовательно ресурса, в частности, электронного практикума по обучению информационной безопасности, как основного педагогического средства формирования умений по защите персональных данных в сети Интернет у студентов колледжа при преподавании специальных дисциплин, структура которого должна способствовать системному, целостному и обозримому отражению содержания образования в области информационной безопасности, и адекватного восприятия его обучающимися.

Анализ направленности и содержания информационной подготовки студентов колледжа, как основного средства формирования фундамента умений в области защиты персональных данных в сети Интернет, позволяет выделить две группы *противоречий,* касающихся как информационной подготовки в целом, так и аспектов информационной безопасности, как её инварианта, в частности. В *первой* из них следует рассматривать противоречия, возникающие между:

1) темпами роста и обновления информационных ресурсов, развития и совершенствования современных информационных и коммуникационных технологий и возможностями их эффективного использования в сферах образования и профессиональной деятельности, ограниченными недостаточной информационной подготовкой.

Вторая группа противоречий обусловлена:

2) несоответствием значимости вопросов информационной безопасности и уровнем педагогического обеспечения их изучения в рамках информационного образования и информационной подготовки, отсутствием соответствующей современным требованиям системы обучения информационной безопасности студентов колледжа.

Проблема исследования заключается в недостаточной разработанности теории и методологических подходов к обучению

основам информационной безопасности студентов колледжа, обучающихся по специальностям, не входящим в группу специальностей по информационной безопасности, ограниченному внедрению проблематики информационной безопасности в информационную подготовку как её обязательного и значимого инварианта в формировании умений в данной области.

В связи с этим тема нашего исследования является актуальной.

Целью исследования является теоретическое обоснование и экспериментальная проверка применения электронного практикума, способствующего эффективному формированию умений по защите персональных данных в сети Интернет у студентов колледжа при преподавании специальных дисциплин.

Объект исследования - образовательный процесс в организации СПО.

Предметом исследования является формирование умений по защите персональных данных в сети Интернет у студентов колледжа при преподавании специальных дисциплин.

Гипотеза исследования: основана на предположении о том, что процесс подготовки студентов колледжа в области защиты персональных данных в сети Интернет будет целостным и результативным, если разработать и внедрить электронный практикум по теме «Защита персональных данных в сети Интернет», способствующий значимому повышению динамики формирования умений в области информационной безопасности.

В соответствии с целью, объектом, предметом и гипотезой определены следующие *задачи исследования:*

1. Раскрыть понятие умений в педагогической практике.

2. Изучить состояние проблемы и опыт обучения информационной безопасности студентов колледжа при преподавании специальных дисциплин.

3. Охарактеризовать существующую систему подготовки в области информационной безопасности студентов колледжа.

4. Разработать и применить электронный практикум для формирования умений по защите персональных данных в сети Интернет у студентов колледжа.

5. Осуществить апробацию разработанного электронного практикума на базе ГБПОУ «Южно-Уральский государственный технический колледж».

Методологическую основу исследования составили:

− системного подхода (Ю.К. Бабанский, А.П. Беляев, В.П. Беспалько, С.М. Маркова, Ю.Н. Петров, В.А. Сластенин, Н.Ф. Талызина);

− разработки и использования автоматизированных обучающих систем в образовании (С.Г. Данилюк, А.Д. Дараган, В.Л. Латышев, Ю.А. Романенко, В.И. Сердюков и др.);

− аспекты нормативно-правового обеспечения информационной безопасности (В.М. Алексеев, Ю.М. Батурин, В.С. Горбатов, О.А. Городов, Р.И. Дремлюга, Ю.А. Журавлев, Г.О. Крылов и др.);

− практические аспекты информационной безопасности и защиты информации (В.А. Галатенко, А.П. Даньков, В.Е. Козлов, А.А. Круглов, А.В. Крысин, В.В. Минин и др.);

− на определение методологических подходов к совершенствованию процесса формирования профессиональных умений студентов оказали влияние концепции формирования профессиональных умений студентов в контексте их профессионального становления (Э.Ф. Зеер, А.М. Новиков, З.А. Решетова, А.Л. Фатыхова, Н.Е. Эрганова).

Теоретическую основу исследования составляют работы:

− теории защиты информации (Е.П. Велихов, Н. Винер, В.А. Герасименко, В.М. Глушков, А.Н. Колмогоров, Л. Дж. Хоффман, К. Шеннон).

− особенности формирования профессиональных умений студентов посредством совершенствования компонентов образовательного пространства (Э.Ф. Зеер, М.В. Мазо, А.М. Новиков, В.А. Скакун, Н.Е. Эрганова).

В процессе работы использовались методы как теоретического, так и эмпирического исследования. Теоретический анализ и синтез психологической, педагогической и методической литературы позволил сформулировать исходные позиции исследования.

Научная новизна исследования заключается в следующем:

1. Раскрыта система обучения студентов колледжа, способствующая подготовке и проведению занятий по информационной безопасности.

2. Разработан электронный практикум по теме «Защита персональных данных в сети Интернет» в рамках дисциплины «Информационная безопасность».

Теоретическая значимость исследования заключается в следующем: в результате комплексного исследования процесса обучения студентов колледжа проанализирована система обучения информационной безопасности, которая является новым теоретическим знанием, обеспечивающим разрешение противоречий, возникших на современном этапе развития информационной культуры и информационной подготовки специалистов среднего звена.

Практическая значимость работы заключается в разработке и применении электронного практикума по теме «Защита персональных данных в сети Интернет» как средства формирования умений по защите персональных данных в сети Интернет у студентов колледжа при преподавании специальных дисциплин (Информационная безопасность).

База исследования: ГБПОУ «Южно-Уральский государственный технический колледж», г. Челябинск, ул. Гагарина, 7.

Апробация результатов исследования и их внедрение. Ход исследования и его результаты докладывались и обсуждались: на

международных конференциях «Инновационные технологии в подготовке современных профессиональных кадров: опыт, проблемы», 2022 г.; «Фундаментальные научные исследования: теория и практика», 2024 г.

Структура магистерской диссертации: введение, две главы, выводы по главам, заключение, список использованных источников, включающий 46 источников, 7 таблиц, 11 рисунков.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ПРОБЛЕМЫ ФОРМИРОВАНИЯ УМЕНИЙ В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СЕТИ ИНТЕРНЕТ У СТУДЕНТОВ КОЛЛЕДЖА

1.1 Понятие умений в педагогической практике среднего профессионального образования

Развитие умений и навыков сопровождает нас всю жизнь и напрямую влияет на успешность и качество жизни человека. Кто-то останавливается в своем развитии практически сразу после школы или вуза, другие же постоянно чему-то учатся и приобретают все новые умения.

Многие ученые утверждают, что умения – это способность выполнять какую-либо деятельность на профессиональном уровне, при этом навыки только дают базу для их формирования. Однако существует и другое мнение: умение – это просто способность выполнять ту или иную операцию, предшествующую навыку. Считается, что навык – это совершенная стадия овладевания тем или иным действием.

Кроме того, есть и третья позиция ученых, которые уверены, что навык приобретается в результате трудовой деятельности, самосовершенствования. Умение же они рассматривают как развитые природные способности и склонности.

О соотношении умений и навыков высказываются различные мнения. Одни исследователи считают, что навыки предшествуют умениям, другие полагают, что умения возникают раньше навыков. Причиной этих разногласий является многозначность слова «умение».

При рассмотрении термина «умения» в психолого-педагогической литературе однозначная интерпретация понятия отсутствует. В частности, в «Большой современной энциклопедии» «умение» определяется как

освоенный человеком способ выполнения действия, который обеспечивается комплексом накопленных знаний и навыков [1].

М.А. Данилов и Б.П. Есипов называют умения определенной подготовленностью к быстрому, точному и сознательному выполнению практических и теоретических действий на основе жизненного опыта и уже приобретенных знаний [2].

В.П. Усачев и Б.М. Бим-Бад идентифицируют умения как способность ребенка осуществлять умственные и практические действия на основе сформированных знаний [3; 4].

Некоторые исследователи понимают под умениями возможности выполнения на профессиональном уровне какой-либо деятельности, отмечая при этом, что умения формируются на базе нескольких навыков.

Умение всегда связано с применением знаний на практике и в процессе учебно-производственной деятельности. Умение формируется путем упражнений и создает возможность выполнения действия не только в привычных, но и в изменившихся условиях.

По своей сути умение — это экстериоризация, т. е. воплощение знаний и навыков в реальные действия. Попадая в новые условия или взаимодействуя с новыми объектами, человек использует имеющиеся у него знания и навыки. В данном случае этот перенос навыков и рассматривается как умения. Умения относятся к навыкам так же, как программа действия к его реализации. Умения шире навыков, они предполагают разные варианты действий.

Таким образом, умение – это готовность человека выполнять определенные действия эффективно и успешно, на основании полученных ранее знаний.

Умения имеют огромное значение в развитии общества, человечества. Они делают человека самостоятельным, приносят ему новые знания, умения, формируют уверенность. Поэтому формирование умений является важной педагогической задачей.

Формирование — это процесс превращения содержания педагогического процесса в результат. Умение, являясь сначала одним из элементов содержания педагогического процесса, усваиваясь, становится результатом.

Формирование умений в педагогике – это процесс закрепления и углубления полученных знаний.

Формирование знаний, навыков и умений протекает оптимально, когда строится на общих дидактических принципах с учетом особенностей содержания учебных дисциплин, групп обучаемых, индивидуальности отдельных из них и при использовании необходимых средств.

Формирование умений осуществляется на основании усвоенных понятий о предмете (объекте или явлении), посредством выполнения разнообразных упражнений, задач и заданий.

Формирование умений во многом зависит от тех условий, которые созданы для обучения, организации процесса выполнения тренировочных задач и упражнений, индивидуальных особенностей (возможностей) обучающегося. Индивидуальные возможности обучающегося играют ведущую роль в усвоении знаний и последующем формировании умений. К индивидуальным особенностям относятся:

- тип нервной системы;
- имеющийся опыт (практический, жизненный);
- уровень теоретических знаний;
- наклонности и способности;
- осознание обучающимся цели и задач обучения;
- уровень понимания содержания обучения и способов овладения умениями.

Основа получения умений заключается в выполнении мыслительной деятельности, в процессе решения различных задач и упражнений, разрешения проблемных ситуаций. В результате мыслительной

деятельности происходит преобразование объекта, выделение его новых свойств и сторон, закрепление основных понятий.

Осуществление мыслительного процесса происходит с помощью выполнения ряда операций, таких как синтез, анализ, абстрагирование, обобщение. Все операции осуществляются вплоть до момента нахождения той стороны объекта, которая наиболее существенна для решения поставленной задачи. При этом, каждый этап открывает перед обучающимся все новые и новые стороны объекта, заставляет его мышление двигаться вперед, предопределяет следующий шаг в решении. Таким образом, новые стороны объекта находят отражение в новых понятиях, а мышление протекает в виде многократной переформулировки решаемой задачи.

Каждая последующая переформулировка задачи – это результат анализа и синтеза данных, которые были получены на предыдущем этапе, выраженный в понятиях, являющихся отражением существенных свойств объекта.

Таким образом, новые формулировки и получаемые сведения об объекте являются движущей силой мышления. Благодаря синтезу и анализу, в процесс мышления включаются новые понятия и свойства, которые фиксируются, тем самым осуществляется процесс формирования умений.

Общая методика формирования умений эффективна, если обеспечивает прежде всего глубину усвоения знаний.

Умение выполнять действия, которые будут доводиться до машинальности (автоматизма), – простое умение. Оно выступает не целью обучения, а частной задачей первого, аналитико-синтетического, этапа формирования навыков. Сложные умения формируются преимущественно для решения реальных жизненных и профессиональных задач, но распространены и в школьном обучении.

Общая методика формирования умений имеет сходство с методикой формирования навыков, но имеет и свои отличия:

– по своей структуре большинство умений сложнее навыков. Алгоритм умений – гибкий: действия и операции могут выполняться иначе, может меняться их последовательность, какие-то элементы – выпадать, какие-то, напротив, – включаться. Поэтому особое внимание уделяется осмысленности, обоснованности всех действий (что, как, в какой последовательности и почему надо делать, и менять по обстановке);

– на аналитико-синтетическом этапе по необходимости отрабатываются некоторые операции и приемы, входящие в структуру умения, выполнение части которых доводится до автоматизма (навыка);

– на этапе автоматизации умения нет, а вместо него после овладения основной структурой действия наступает этап выполнения действий в «штатных» – наиболее вероятных (трех-семи) ситуациях;

– на этапе разнообразия и гибкости, когда условия выполнения действия приобретают разнообразность (начиная с ситуации, находящейся между штатными). Обучающихся учат решать одну и ту же задачу в постоянно меняющихся условиях, требующих от них видоизменять порядок действия, исключать одни способы и операции и заменять их другими. Предъявляются требования к самостоятельному, творческому, обоснованному видоизменению действий и выборам в новых условиях;

– важнейшие значение придается последнему этапу – надежности умения. Это специфичный и исключительно важный для формирования этап. По нарастающей усложняются и множатся новизна, неожиданность, скорость изменений, значимость, рискованность, опасность, повышенная ответственность, противодействие, повышение вероятности неудач и т.д. Обучающие учатся наблюдать, мыслить, оценивать, действовать самостоятельно, проявлять находчивость, разумность, достигать нужного результата, несмотря на новизну, необычность, неожиданность возникающей ситуации. Сложность обстановки и трудности в конце

формирования умения приближаются к неопределенным, в которых обучаемых учат принимать наилучшие решения. Повышенное значение придается разбору упражнений, обсуждению действий, совместному поиску оптимального и обоснованного варианта.

Таким образом, формирование умения может происходить так:

1. Обучающиеся получают знания, на основании которых в последующем педагогом ставится учебная задача. То есть, алгоритм такой: знания – задачи – применение знаний (формирование умений).

2. Обучающиеся определяют признаки, которые отличают один тип задач от других. В процессе выполнения задания, они определяют тип задачи и выполняют операции, необходимые для решения этого типа задач.

3. Обучающиеся учатся умственной деятельности, необходимой для использования знаний.

1.2 Характеристика существующей системы подготовки в области информационной безопасности студентов колледжа

Тенденции развития мирового сообщества свидетельствуют о возрастании потребностей в специалистах, владеющих новейшими информационными и коммуникационными технологиями, обладающих высокой информационной культурой и умеющих применять в своей профессиональной деятельности знания и навыки по обеспечению информационной безопасности.

По мере развития и углубления многомерных и многовекторных процессов, сопровождающих информатизацию современного общества, возрастает внимание к ее социальным и психологическим аспектам, связанным с необходимостью учета физического, психического и социального начал личности. Все это обусловливает внимание государства и общества к проблемам информационной безопасности, направленное на формирование нормативной базы, совершенствование системы защиты

информации и системы защиты государственной тайны, углубление научных изысканий, организацию подготовки кадров в области информационной безопасности. В частности, по-прежнему актуальной остается задача «создания единой системы подготовки кадров в области информационной безопасности и информационных технологий» [1, с. 18], обеспечивающей не только подготовку квалифицированных специалистов в области информационной безопасности и защиты информации, но и изучение проблематики информационной безопасности всеми другими категориями специалистов, подготавливаемых в системе профессионального образования.

На государственном уровне под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства [1, с.5]. Для обеспечения национальных интересов в информационной сфере выделены четыре составляющих:

– гуманистическая, направленная на обеспечение конституционных прав и свобод личности, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма;

– политическая, включающая информационное обеспечение государственной политики по доведению достоверной информации до российской и международной общественности;

– технологическая, обеспечивающая развитие современных информационных технологий и отечественной индустрии информации;

– секьюритологическая, рассматривающая задачи защиты информационных ресурсов от несанкционированного доступа, обеспечения безопасности использования информационных и телекоммуникационных систем.

В соответствии с вышеперечисленными составляющими деятельности по обеспечению национальных интересов в информационной сфере группируются виды угроз информационной безопасности (ИБ).

Воздействию угроз ИБ РФ наиболее подвержены информационные и учетные автоматизированные системы, обеспечивающие деятельность общества и государства в различных сферах; системы бухгалтерского учета предприятий, учреждений и организаций независимо от формы собственности» [1, с.21].

Таким образом, подготовка в области информационной безопасности и защиты информации для студентов важна и актуальна. Профессиональная деятельность специалистов в различных сферах в условиях жесткой конкурентной борьбы. Взаимодействие конкурентных сил осуществляется в условиях информационного противоборства и применения т.н. информационного оружия, т.е. информация становится важнейшим ресурсом в острой конкурентной борьбе в различных сферах: политической, экономической, духовной, нравственной и т.д.

Кроме того, продолжают действовать и традиционные, существовавшие всегда деструктивные факторы, такие, как хищения, мошенничество, коррупция, промышленный шпионаж, подлоги и др. Острота проблемы информационной безопасности возрастает по мере увеличения масштабов внедрения современных информационных и коммуникационных технологий (ИКТ), являющихся технологической основой процессов глобализации, во все сферы жизнедеятельности современного общества.

По мере развития электронных систем для платежей, расчетов, торговли экономическая деятельность все чаще осуществляется в электронной среде и связана с информационными рисками. Поэтому отсутствие у пользователей надлежащих знаний, умений и навыков в области информационной безопасности чревато серьезными издержками при использовании ИКТ в различных сферах, поскольку одним из

основных сдерживающих факторов их внедрения является принципиальная уязвимость от различного рода угроз информационной безопасности.

Анализ направленности и содержания информационной подготовки студентов различных специальностей позволяет выделить ряд противоречий, касающихся как информационной подготовки в целом, так и аспектов информационной безопасности как ее инварианта, возникающих между:

1) уровнем требований, предъявляемых к индивидууму в постиндустриальном обществе, и уровнем личностной информационной культуры;

2) темпами роста и обновления информационных ресурсов, развития и совершенствования современных ИКТ, а также высокой затратностью их внедрения и возможностями их эффективного использования в сферах образования и профессиональной деятельности, ограниченными недостаточной информационной подготовкой;

3) стандартизацией и унификацией требований к качеству подготовки в области информационных и коммуникационных технологий на различных этапах образования и значительной дифференциацией индивидуальных уровней обученности, недостаточной межэтапной корреляцией программ подготовки в области ИКТ;

4) все более значимой ролью информационной безопасности в профессиональной деятельности в условиях конкурентной среды и недостаточным уровнем реальной компетентности в области информационной безопасности будущих специалистов;

5) несоответствием значимости вопросов информационной безопасности и педагогическим обеспечением их изучения в рамках информационной подготовки.

Характеристики существующей системы подготовки в области информационной безопасности и защиты информации.

В самом общем плане категории специалистов, которым необходима подготовка по информационной безопасности в системе профессионального образования, могут быть сведены в несколько основных групп:

– специалисты в области информационной безопасности и защиты информации: аналитики по компьютерной безопасности, разработчики средств и систем безопасности, сотрудники организаций и подразделений, занимающихся информационной безопасностью и защитой информации, в том числе в системах критических приложений (опасных производств);

– специалисты в области информационных технологий (ИТ-специалисты), обеспечивающие создание и эксплуатацию информационных систем, а также отвечающие за их администрирование и безопасность;

– специалисты, обеспечивающие эксплуатацию сложных иерархических человеко-машинных систем управления специального назначения (эргатических систем);

– все остальные специалисты, имеющие доступ к информационным системам, использующие информационные и коммуникационные технологии как в профессиональной деятельности, так и в интересах самосовершенствования и развития.

При этом каждая из групп может быть дифференцирована в зависимости от условий социального заказа на подготовку специалистов определенного профиля.

Для подготовки первой из перечисленных категорий специалистов, чья профессиональная деятельность напрямую связана с обеспечением информационной безопасности и защиты информации, основополагающим является наличие соответствующих Федеральных государственных образовательных стандартов (ФГОС) и разработанных на их базе основных профессиональных образовательных программ в области информационной

безопасности по специальностям, выделенным в группу 10.00.00 в перечне направлений и специальностей (табл. 1).

Таблица 1 − Перечень специальностей среднего профессионального образования в области информационной безопасности

Коды укрупненных групп специальностей. Коды специальностей	Наименования укрупненных групп специальностей. Наименования специальностей	Квалификация(и) специалиста среднего звена
10.00.00	**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**	
10.02.01	Организация и технология защиты информации	Техник по защите информации Старший техник по защите информации
10.02.02	Информационная безопасность телекоммуникационных систем	Техник по защите информации Старший техник по защите информации
10.02.03	Информационная безопасность автоматизированных систем	Техник по защите информации Старший техник по защите информации
10.02.04	Обеспечение информационной безопасности телекоммуникационных систем	Техник по защите информации
10.02.05	Обеспечение информационной безопасности автоматизированных систем	Техник по защите информации

Подготовка таких специалистов предусматривает изучение общепрофессиональных и специальных дисциплин, охватывающих широкий круг вопросов по обеспечению информационной безопасности и защиты информации.

В таблице 2 представлена дифференциация подготовки по информационной безопасности специалистов в системе среднего профессионального образования.

Таблица 2 − Дифференциация подготовки по информационной безопасности специалистов в системе среднего профессионального образования

№ п/п	Категории выпускников СПО	Качественная характеристика потребности
1.	Специалисты в области информационной безопасности и защиты информации: аналитики по компьютерной безопасности, разработчики средств и систем безопасности, сотрудники органов, организаций и подразделений, занимающихся информационной безопасностью и защитой информации, в том числе в системах критических приложений.	Незначительная
2.	Специалисты, обеспечивающие эксплуатацию сложных иерархических человеко-машинных систем управления специального назначения (эргатических систем).	Незначительная
3.	Специалисты в области информационных технологий (ИТ-специалисты), обеспечивающие создание и эксплуатацию информационных систем, в том числе отвечающие за их администрирование и безопасность.	Существенная
4.	Специалисты, имеющие доступ к информационным системам, использующие информационные и коммуникационные технологии как в профессиональной деятельности, так и в интересах самосовершенствования и развития.	Наиболее значимая

Для подготовки первой категории специалистов, чья профессиональная деятельность напрямую связана с обеспечением информационной безопасности и защиты информации, создана система, основы которой были заложены Решением Межведомственной комиссии Совета безопасности Российской Федерации по информационной безопасности от 28.09.95 г. №8.3, приказом Госкомвуза России от 22.12.95 г. №1687, решением Комитета по образованию и науке Государственной Думы Российской Федерации «О состоянии и перспективах подготовки кадров в области информационной безопасности» от 24.10.96 г. в 90-х годах века минувшего.

Система подготовки специалистов в области информационной безопасности и защиты информации, сформированная на базе Учебно-методического объединения (УМО) вузов России по образованию в области информационной безопасности в системе высшей школы носит

узкопрофессиональный, специализированный характер, и отличается закрытостью. Для целого ряда других министерств и ведомств (в первую очередь силовых) сформированы ведомственные подсистемы подготовки кадров, по своей структуре аналогичные общей системе подготовки специалистов в Министерстве образования и науки Российской Федерации.

Следует отметить, что в системе Федеральной службы безопасности (ФСБ) России, Министерства обороны, Федеральной службы охраны (ФСО), Министерства внутренних дел (МВД), Федеральной службы по техническому и экспортному контролю (ФСТЭК – ранее Гостехкомиссия при Президенте РФ), Министерство путей сообщения (МПС), других министерств и ведомств России сформировались ведомственные подсистемы подготовки кадров, по своей структуре аналогичные общей системе подготовки специалистов в Министерстве образования и науки России. В рамках данных министерств и ведомств имеются образовательные учреждения различного вида, реализующие образовательные программы среднего, высшего, дополнительного и послевузовского профессионального образования в области информационной безопасности. Подобные подсистемы направлены на целевую подготовку кадров в интересах ведомств и по своей организации, содержанию и развитию имеют определенную специфику.

В целях координации работы по подготовке кадров в области информационной безопасности работают Межведомственная комиссия Совета Безопасности Российской Федерации по информационной безопасности (см. Указ Президента Российской Федерации от 29 декабря 2012 г. №1711 «О составе по должностям»), Межведомственная комиссия по защите государственной тайны (см. Указ Президента Российской Федерации от 6 октября 2004 г. №1286), Координационный совет Минобразования России по проблемам подготовки специалистов в области защиты государственной тайны и информационной безопасности.

Подготовка кадров в области информационной безопасности имеет существенные особенности, поскольку выступает не только как реакция на спрос рынка в отношении таких специалистов, но и как важная составляющая комплекса мероприятий государства по противодействию угрозам в информационной сфере. Этими особенностями определяются и содержание подготовки указанных специалистов, и особые требования, предъявляемые к образовательным учреждениям при организации такой подготовки [40].

Специалисты с такой подготовкой в настоящее время полноценно могут готовиться только вне сферы гуманитарного, педагогического, экономического образования, однако уже сегодня нуждается в научной проработке вопрос о введении в существующие экономические специальности специализации по безопасности информационных систем в экономике, направленной на подготовку специалистов с экономическим образованием и высоким уровнем подготовки в области информационной безопасности, ориентированных по предназначению на работу в службах финансового мониторинга, аналитического обеспечения экономической безопасности, решение задач форестики (финансовой разведки).

Для целого ряда других министерств и ведомств сформированы ведомственные подсистемы подготовки кадров, по своей структуре аналогичные общей системе подготовки специалистов в Министерстве образования и науки РФ. Эти подсистемы направлены на целевую подготовку кадров в интересах ведомств и по своей организации, содержанию и развитию имеют определенную специфику. Взаимодействие подсистем осуществляется в рамках Координационного совета министерства по проблемам подготовки кадров в области защиты государственной тайны и информационной безопасности, созданного приказом министра образования РФ от 25.02.2003 г. [2].

Вопросы информационной безопасности с той или иной степенью полноты и детализации нашли отражение в учебных планах и программах

подготовки специалистов среднего звена 09.02.07 Информационные системы и программирования, и других категорий ИТ-специалистов. Помимо изучения проблематики информационной безопасности и защиты информации в рамках дисциплин информационного цикла их знания в этой области развиваются и систематизируются в рамках общепрофессиональных и специальных дисциплин соответствующей направленности.

Для самой широкой категории специалистов, являющихся конечными пользователями современных ИКТ весь спектр вопросов по информационной безопасности в настоящее время сконцентрирован в курсе информатики и Информационных технологий в профессиональной деятельности, что существенно сужает рассмотрение проблемы и нуждается в корректировке.

Как отмечается в [8; 9; 27; 46] важнейшей задачей является усиление подготовки специалистов по информационной безопасности гуманитарного профиля.

Особую остроту приобретает гуманистическая составляющая проблемы ИБ, предполагающая наличие адекватного гражданского воспитания и основанная в т.ч. на информационном праве, высокой информационной культуре.

Для создания системы подготовки по информационной безопасности последняя должна быть определена как педагогическая категория. Под категорией в философии, например, понимается наиболее общее и существенное понятие, выражающее одну из основных форм или одно из основных отношений бытия (материя, время, пространство и т.п.); категории общепсихологические представляют собой предельно широкие психологические понятия (сознание, личность, деятельность и т.п.); в педагогике это должны быть понятия, отображающие существенные ее стороны как науки о сущности развития и формирования человеческой личности. В этом ключе педагогическая категория «подготовка по

информационной безопасности» может трактоваться как обязательный компонент информационной подготовки, обеспечивающий секьюритологический аспект информационной культуры, характеризующий состояние защищенности инфосферы индивидуума в процессе информационного взаимодействия от различного рода информационных опасностей и угроз, а также регламентирующий работу индивидуума с информационными ресурсами с соблюдением морально-этических и правовых норм.

Для решения задачи обучения основам информационной безопасности и защиты информации как инвариантной составляющей информационной подготовки, направленной на формирование информационной культуры личности на этапе перехода к постиндустриальному обществу, требуется системный подход, реализующий методологические, организационные, содержательные, дидактические и технологические аспекты.

Одним из основополагающих принципов такого подхода является преемственность между уровнями образования. Система подготовки в области информационной безопасности и защиты информации должна быть детерминирована по всем уровням образовательной деятельности как общего (пропедевтика, т.е. вводный курс, а также базовый и профильный курсы информатики), так и профессионального образования – среднего, высшего, послевузовского и дополнительного.

В процессе информационной подготовки на этапе общего образования закладываются основы компьютерной грамотности и компьютерной компетентности как фундамент информационной культуры личности. В стандарте основного общего образования по информатике и информационным технологиям отмечается, что «изучение информатики и информационных технологий в основной школе должно быть направлено на воспитание ответственного отношения к информации с учетом правовых и этических аспектов ее распространения; избирательного

отношения к полученной информации». А в обязательный минимум основных образовательных программ включены дидактические единицы, рассматривающие информационные процессы в обществе («информационные ресурсы общества, образовательные информационные ресурсы; личная информация, информационная безопасность, информационные этика и право»). В требованиях к уровню подготовки выпускников школы учтены их умения по применению мер антивирусной безопасности, использованию приобретенных знаний и умений на практике.

Актуальными остаются задачи повышения правовой грамотности в вопросах использования средств информационных и коммуникационных технологий, применения типовых методов защиты информации при работе на персональном компьютере, в локальных и глобальных сетях. Поэтому подготовка в области информационной безопасности и защиты информации нуждается в существенном совершенствовании и развитии на последующих этапах образования.

Модель системы подготовки будущих специалистов гуманитарного профиля средствами информационных технологий раскрывает теоретическую сущность целостного образовательного процесса, построенного на идее формирования информационной культуры и информационной безопасности.

Система подготовки должна характеризоваться комплексностью, непрерывностью, технологичностью (см. рис. 1). Содержание обучения основам информационной безопасности и защиты информации может быть построено на основе системного анализа основных объектов предметной области будущей профессиональной деятельности. Результатом такого анализа должно стать выявление базовых объектов изучения, их взаимосвязей (процессов взаимодействия), методов и технологии их изучения. При проектировании системы подготовки специалистов гуманитарного профиля средствами информационных

технологий с учетом информационной безопасности должны быть использованы основополагающие принципы архитектоники – научность; преемственность; последовательность; систематичность; доступность; связь теории с практикой; адаптивность и динамичность; полифункциональность [3].

Рисунок 1 − Модель системы обучения основам информационной безопасности

Целями обучения в такой системе является подготовка к профессиональной деятельности в соответствии с требованиями ФГОС, а также формирование высокого уровня информационной культуры и подготовки в области информационной безопасности.

Проблематика информационной безопасности должна стать органической частью информационной подготовки специалистов гуманитарного профиля, необходимым компонентом формирования информационной культуры личности в условиях постиндустриального общества.

Таким образом, глубокое понимание проблематики информационной безопасности подготавливаемыми в системе среднего профессионального образования специалистами может быть достигнуто образовательной деятельностью по нескольким взаимодополняющим направлениям:

- получением базового образования в области информационной безопасности в рамках существующих специальностей (см. табл. 1);
- получением второго высшего образования (объем вновь изучаемого материала по проблематике информационной безопасности – несколько тысяч часов);
- прохождением профессиональной переподготовки или получением дополнительной квалификации (объем вновь изучаемого дополнительного материала – в рамках тысячи часов и более);
- формированием специализации по информационной безопасности в рамках специальности высшего образования (объем вновь изучаемого материала также составляет несколько сот часов, но не дополнительно, а взамен);
- внедрением во все специальности, не относящиеся к группе специальностей «Информационная безопасность» отдельной одноименной дисциплины;
- совершенствованием информационной подготовки специалистов в области информационной безопасности за счет введения в

соответствующие Федеральные государственные образовательные стандарты высшего и среднего профессионального образования дидактических единиц, объективно отражающих значимость и научный уровень решения этой проблемы, создания и укрепления внутри дисциплинарных связей дисциплин информационного цикла и междисциплинарных связей с дисциплинами других разделов.

1.3 Дидактические особенности содержательной линии по защите персональных данных в Интернете при преподавании специальных дисциплин

В качестве содержательных линий информационной безопасности в информационной подготовке, согласно педагогическому опыту, мы будем рассматривать структуру содержания обучения.

Применительно к содержательным линиям системообразующего курса «Информационная безопасность» актуальным является их определение С.А. Бешенковым, как «устойчивых единиц содержания обучения, образующих каркас курса, его архитектонику» [11].

Содержание обучения рассматривается нами как системообразующий элемент в методической системе обучения информационной безопасности, компоненты которого не только соответствуют основным знаниям и умениям будущего специалиста в соответствии с его квалификационной характеристикой, указанной в соответствующем Федеральном государственном образовательном стандарте среднего профессионального образования, но и отвечает за наполнение каждого из них конкретными понятиями согласно содержательным линиям обучения, которые, в свою очередь, предопределяют основные разделы содержания обучения, реализуют основную доминанту в обучении и позволяют, согласно этой доминанте, выстраивать изложение учебного материала, а также изучение базовых

понятий и всего цикла учебных дисциплин в рамках, например, предметной или специальной подготовки обучающихся.

Как уже отмечалось выше, информационная подготовка студентов должна строиться в соответствии с профессиональными требованиями, отраженными в соответствующих профилю и направлению подготовки Федеральных государственных образовательных стандартах и профессиональных стандартах.

Особую остроту приобретает гуманистическая составляющая проблемы информационной безопасности, предполагающая при подготовке специалистов решение задач «защиты от информации», адекватного гражданского воспитания, основанного, в т.ч. на информационном праве, высокой информационной культуры.

Компонентами системы обучения основам информационной безопасности являются цели и ожидаемые результаты обучения, содержание обучения и методическое обеспечение, включающее методы, организационные формы и средства обучения.

В свою очередь, компонентами содержания обучения по информационной безопасности выступают знания, накопленные в этой предметной области (научно обоснованные факты, дефиниции, законы и закономерности, гипотезы и теории), опыт осуществления способов деятельности по обеспечению информационной безопасности и защиты информации. Архитектоника содержания подготовки будет определяться соответствующими содержательными линиями.

Структурно детерминированная модель содержания обучения основам информационной безопасности может быть построена на основе системного анализа основных объектов предметной области будущей профессиональной деятельности обучающихся, соотнесенных с матрицей опасностей и угроз для выявленных информационных процессов. Результатом такого анализа должно стать выявление базовых объектов

изучения, их взаимосвязей (процессов взаимодействия), методов и технологии их изучения.

Дидактические особенности содержательной линии по защите персональных данных в Интернете при преподавании специальных дисциплин имеют свои особенности и требуют учета следующих факторов:

1. При преподавании защиты персональных данных в Интернете необходимо учитывать уровень знаний и навыков студентов. Некоторые студенты могут иметь базовые знания в этой области, в то время как другие могут быть новичками. Поэтому важно адаптировать содержание и методики обучения к уровню знаний студентов.

2. Практическая направленность. Обучение защите персональных данных в Интернете должно быть практически ориентированным. Студенты должны получать не только теоретические знания, но и практические навыки, которые помогут им применять правила безопасности в реальной жизни.

3. Интерактивные методы обучения. Для эффективного обучения защите персональных данных в Интернете рекомендуется использовать интерактивные методы обучения, такие как дискуссии, групповые проекты, ролевые игры и т.д. Эти методы помогают студентам активно взаимодействовать с материалом и лучше усваивать информацию.

4. Регулярное обновление содержания. В связи с быстрым развитием информационных технологий и появлением новых угроз безопасности, важно регулярно обновлять содержание обучения. Это позволяет студентам быть в курсе последних тенденций и технологий в области защиты персональных данных.

Для более эффективного обучения студентов рекомендуется интегрировать обучение защите персональных данных с реальными проектами и задачами. Это позволяет студентам применять полученные знания на практике и лучше усваивать материал. Также, для эффективного обучения важно предоставлять студентам обратную связь и оценку их знаний

и навыков. Это помогает студентам понимать свои сильные и слабые стороны и улучшать свои навыки в области защиты персональных данных.

Для углубления знаний и навыков в области информационной безопасности в рамках дисциплин «Информатика» и «Информационные технологии в профессиональной деятельности» необходимо, с учетом интегративного подхода, использовать имеющиеся внутрипредметные связи, прослеживаемые между традиционными разделами информатики и проблематикой информационной безопасности, акцентируя внимание на таких вопросах, как безопасность операционных систем, безопасность офисных приложений, безопасность в базах данных, безопасность при работе в локальных и глобальных сетях и т.п. (табл. 3).

Таблица 3 − Вопросы информационной безопасности в дисциплинах информационного цикла

№ п/п	Темы дисциплин информационного цикла	Вопросы информационной безопасности
	Операционные системы	Средства обеспечения информационной безопасности (идентификация и аутентификация, профили пользователей, разрешение доступа к папкам и файлам, передача прав владения, шифрующие файловые системы, использование служебных программ, групповых политик, сертификатов, средств мониторинга системы)
	Офисные приложения	Доступ к файлам по паролю, открытие документов по паролю или только для чтения, защита книги, листа, ячейки, раздела документа от изменений, использование шаблонов, шифрование баз данных, использование цифровой подписи
	Работа в Интернет	Настройки безопасности, настройки браузеров, защита от спама, использование антивирусных средств, операции с цифровой подписью
	Информационные системы	Меры обеспечения информационной безопасности при работе с профессиональными информационными системами

Несмотря на жесткие временные рамки реализации учебных планов по информатике и информационным технологиям, тематика информационной безопасности должна найти в нем соответствующее ее значимости место в подготовке обучающихся, в том числе и с учетом резервов самостоятельной работы студентов. При этом качество

подготовки может быть улучшено за счет более эффективного использования внутрипредметных связей.

При подготовке в области обеспечения информационной безопасности также должны эффективно использоваться межпредметные связи, устанавливающие корреляцию дисциплин информационного цикла с другими областями:

1) в области общих гуманитарных и социально-экономических дисциплин – философия, социология, политология, культурология, право (для освещения роли и значения информации и информационных ресурсов в современном обществе, в том числе для обеспечения прав и свобод личности, важности их гуманитарного, морально-этического, культурологического, правового аспектов);

2) в области общих математических и естественнонаучных дисциплин – математика и ее приложения (для освещения вопросов о применении математических методов преобразования данных с целью их защиты);

3) в области общепрофессиональных и специальных дисциплин должны найти адекватное отражение аспекты безопасности хозяйственной деятельности в электронной среде.

Для укрепления межпредметных связей в состав изучаемых дисциплин могут быть включены дисциплины, конкретизирующие и углубляющие такое взаимодействие. Учебная дисциплина «Информационная безопасность» как системообразующий элемент подготовки по информационной безопасности. Несмотря на междисциплинарный характер проблемы информационной безопасности, в состав изучаемых курсов должна быть включена дисциплина «Информационная безопасность», главная цель которой – повышение эффективности подготовки специалистов по обеспечению информационной безопасности при использовании ИКТ в сфере профессиональной деятельности.

Наряду с традиционно рассматриваемыми аспектами ИБ и защиты информации в ней должны найти отражение методологические, социально-философские, культурологические, правовые, организационно-управленческие аспекты информационной безопасности [4].

Данная учебная дисциплина должна дать обучаемым комплекс сведений о со временного состояния проблемы обеспечения информационной безопасности применительно к сфере будущей деятельности подготавливаемого специалиста, существующих угрозах, видах обеспечения ИБ, методах и средствах защиты информации, основах построения систем защиты. Особое место должны занимать правовой и морально-этический аспекты обеспечения информационной безопасности.

В утвержденных Министерством образования РФ примерных Федеральных образовательных государственных стандартах по дисциплине «Информационные технологии профессиональной деятельности» для раздела «Основные угрозы и методы обеспечения информационной безопасности» дидактические единицы могут быть сведены в три основные группы, ориентированные на различные аспекты ИБ, что вполне корреспондирует с положениями Доктрины информационной безопасности РФ (табл. 4).

Таблица 4 − Аспекты информационной безопасности в подготовке студентов колледжа

Социальные аспекты	Правовые аспекты	Технологические и секьюритологические аспекты
1.Информационная структура РФ 2.Информационная безопасность и ее составляющие 3. Угрозы безопасности информации и их классификация 4.Основные виды защищаемой информации 5.Проблемы информационной безопасности в мировом сообществе	1. Законодательные и иные правовые акты РФ, регулирующие правовые отношения в сфере информационной безопасности и защиты государственной тайны 2. Система органов обеспечения ИБ в РФ 3. Административно-правовая и уголовная ответственность в информационной сфере	1. Защита от несанкционированного вмешательства в информационные процессы 2. Организационные меры, инженерно-технические и иные методы защиты информации. 3. Защита информации в сетях, антивирусная защита 4. Специфика обработки конфиденциальной информации в компьютерных системах

Такая декомпозиция позволяет сформировать и наполнить подготовку в области информационной безопасности прежде всего социальным содержанием, поскольку именно социальные аспекты информационной безопасности носят гносеологический основополагающий характер. Их изучение позволяет выявить значимость проблемы ИБ как на цивилизационном, так и на личностном уровне в полном соответствии с гуманитарной составляющей информационной безопасности.

В результате изучения учебных вопросов этого блока обучаемые должны знать суть проблемы обеспечения информационной безопасности и ее особенности, основные угрозы для информационных ресурсов во всех социально значимых областях человеческой деятельности, роль человеческого фактора в решении задач обеспечения информационной безопасности. Именно люди составляют наиболее уязвимый «компонент» информационных ресурсов и представляют наибольшую опасность для них как в корпоративной среде, так и при индивидуальном использовании информационных и коммуникационных технологий. Поэтому среди направлений решения проблемы информационной безопасности, таких, как создание безопасных операционных систем и приложений, улучшение средств защиты, совершенствование законодательной базы, – важную роль играет система просвещения (образования).

В контексте информационной безопасности должны быть рассмотрены проблемы компьютерной этики, возникающие в связи с отсутствием ясности в вопросах о том, каковы же этические ограничения при применении компьютерных технологий. Одним из основных результатов изучения социальных аспектов информационной безопасности должно быть осознание обучаемыми того обстоятельства, что безопасность информационных систем и технологий не является их врожденным, эмерджентным свойством, а является следствием диалектического взаимодействия деструктивных факторов (угроз и

опасностей различной этимологии) и механизмов комплексной системы защиты информации, обеспечивающей их предотвращение, блокирование, устранение, минимизацию рисков.

Обязательным компонентом подготовки по информационной безопасности является изучение основ ее правового обеспечения. В числе задач, решаемых государством в сфере обеспечения информационной безопасности, является интенсивное развитие правового регулирования отношений в области противодействия угрозам; закрепляются приоритетные интересы в информационной сфере, чему способствует принятие соответствующих законодательных актов. Это предопределяет обязательность изучения основ правового обеспечения информационной безопасности, содержательным наполнением которого должно стать представление о сложностях правового регулирования отношений в информационной сфере, обусловленных самим понятием «информация», отсутствием единства его толкования в юриспруденции. В контексте информационного права должны изучаться аспекты информационной безопасности в системе национальной и экономической безопасности страны, соответствующие конституционные нормы и правовые акты, а также уровни правового регулирования в области информационной безопасности.

В рамках изучения технологических и секьюритологических аспектов обеспечения информационной безопасности компьютерных систем и технологий предметом изучения должны стать принципы и содержание организационного обеспечения информационной безопасности (политика безопасности, контроль, разграничение и ограничение доступа к информационным ресурсам); принципы создания комплексных систем защиты информации; методы и средства обеспечения информационной безопасности (аутентификация и идентификация пользователей и технических средств, организация защиты информации в персональных компьютерах, криптографическое преобразование

информации и электронная подпись); особенности защиты информации в базах данных и в сетях телекоммуникаций; основы компьютерной вирусологии, методы и средства защиты от компьютерных вирусов и вредоносных программ; требования к пользователям и рекомендации по обеспечению личной информационной безопасности.

Для углубления знаний и навыков в области информационной безопасности в рамках дисциплин «Информатика» и «Информационные технологии в профессиональной деятельности» необходимо, с учетом интегративного подхода, использовать имеющиеся внутрипредметные связи, прослеживаемые между традиционными разделами информатики и проблематикой информационной безопасности, акцентируя внимание на таких вопросах, как безопасность операционных систем и офисных приложений, безопасность в базах данных, безопасность при работе в локальных и глобальных сетях и т.п.

Несмотря на жесткие временные рамки реализации учебных планов по данным дисциплинам, тематика ИБ должна найти соответствующее ее значимости место в подготовке будущих специалистов, в том числе и с учетом резервов самостоятельной работы студентов.

При этом качество подготовки может быть улучшено за счет более эффективного использования внутрипредметных связей. Основным в построении «технологического блока» является его структуризация и такой отбор содержания, который обеспечил бы понимание обучаемыми того обстоятельства, что, несмотря на множество опасностей и угроз, возможно поддержание необходимого и достаточного уровня информационной безопасности и минимизации рисков при соответствующей организации, вложении средств и уровне подготовки пользователей.

Одним из важных направлений развития системы обучения является разработка деятельностного компонента содержания, т.е. включения в обязательный минимум содержания образования специально отобранных

способов деятельности, техник и технологий, ключевых компетенций и иных процедурных элементов, которыми необходимо овладеть обучающимся. В рамках совершенствования среднего профессионального образования, особое внимание уделяется компетенциям, т.е. умению применять полученные теоретические знания, умения и навыки для решения задач в предметной области. Поэтому обязательным компонентом в системе обучения студентов колледжа должен стать электронный практикум по информационной безопасности.

Выводы по Главе I

В первой главе «Теоретические аспекты проблемы формирования умений в области защиты персональных данных в сети Интернет у студентов колледжа» раскрыто понятие «умения», проведен анализ нормативно-методической документации подготовки студентов колледжа, современное состояние и педагогические аспекты проблемы информационной безопасности в контексте глобальной информатизации современного общества.

1. Умение – это готовность человека выполнять определенные действия эффективно и успешно, на основании полученных ранее знаний. Умения имеют огромное значение в развитии общества, человечества. Они делают человека самостоятельным, приносят ему новые знания, умения, формируют уверенность. Поэтому формирование умений является важной педагогической задачей. Формирование умений во многом зависит от тех условий, которые созданы для обучения, организации процесса выполнения тренировочных задач и упражнений, индивидуальных особенностей (возможностей) обучающегося.

Формирование умений в области информационной безопасности студентов колледжа может быть достигнуты путем введения в соответствующие стандарты образования соответствующих компетенций, направленных на формирование информационной культуры специалиста с

обязательной составляющей – компетентностью в области информационной безопасности или профессиональных умений в данной области.

2. Подготовка в области информационной безопасности и защиты информации для студентов важна и актуальна. Вопросы информационной безопасности с той или иной степенью полноты и детализации нашли отражение в учебных планах и программах подготовки специалистов среднего звена 09.02.07 Информационные системы и программирования, и других категорий ИТ-специалистов. Помимо изучения проблематики информационной безопасности и защиты информации в рамках дисциплин информационного цикла их знания в этой области развиваются и систематизируются в рамках общепрофессиональных и специальных дисциплин соответствующей направленности. Для самой широкой категории специалистов, являющихся конечными пользователями современных ИКТ весь спектр вопросов по информационной безопасности в настоящее время сконцентрирован в дисциплинах «Информатика» и «Информационных технологий в профессиональной деятельности», что существенно сужает рассмотрение проблемы и нуждается в корректировке.

Формирование умений по защите персональных данных должно быть интегрировано в учебный процесс колледжа. Это может быть достигнуто через включение соответствующих тем в учебные планы и программы, проведение практических занятий и проектов, а также использование специализированных учебных материалов и ресурсов.

3. Дидактические особенности содержательной линии по защите персональных данных в Интернете при преподавании специальных дисциплин имеют свои особенности и требуют учета следующих факторов: необходимо учитывать уровень знаний и навыков студентов; практическая направленность; регулярное обновление содержания обучения, что позволит студентам быть в курсе последних тенденций и технологий в области защиты персональных данных.

ГЛАВА 2. РАЗРАБОТКА ЭЛЕКТРОННОГО ПРАКТИКУМА КАК СРЕДСТВА ФОРМИРОВАНИЯ УМЕНИЙ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В СЕТИ ИНТЕРНЕТ У СТУДЕНТОВ КОЛЛЕДЖА

2.1 Методологические принципы разработки и внедрения электронного практикума для формирования умений в области защиты персональных данных в сети Интернет

Электронный практикум по теме «Защита персональных данных в сети Интернет» должен соответствовать целому ряду требований:

- наличие механизма приобретения знаний по информационной безопасности;
- наличие возможности обратной связи с обучаемым;
- возможность адаптации к обучаемому;
- наличие инструментов, для настройки электронного практикума на предметную область за счёт внесения в нее учебной информации;
- наличие средств входного контроля для предварительного определения уровня подготовки и способностей обучаемого и соответствующей самонастройки ЭП на определенный уровень;
- присутствие средств создания и применения стратегий обучения и моделей обучаемого;
- наличие средств контроля процесса обучения.

Реализация этих основных требований представляет сложный и трудоемкий процесс, поэтому даже наиболее совершенные электронные образовательные ресурсы соответствуют лишь некоторым из указанных требований.

Требования, предъявляемые к электронным средствам обучения, во многом определяют эффективность обучения с использованием электронных средств обучения.

Эффективность применения электронного практикума в учебном процессе для студентов колледжа, возможно, определить, сравнивая результаты обучения с применением электронного практикума и без его использования.

В общем случае эффективность, применительно к учебному процессу, обычно рассматривается как определенный результат достижения поставленной конкретной цели, поэтому в качестве целевых показателей эффективности электронного практикума следует рассматривать следующее:

- рационализация процесса обучения во всех его формах для повышения качества подготовки студентов колледжа;
- оценка влияния различных средств обучения на качество учебного процесса.

Применительно к электронным средствам обучения, первая цель характеризует эффективность его функционирования, а вторая - влияние электронного средства обучения на повышение качества учебного процесса.

Мерами эффективности или показателями качества функционирования электронного практикума являются:

- развитие творческой активности студентов в процессе обучения;
- адаптация электронного практикума к индивидуальным характеристикам студентов;
- многофункциональность применения и использование в различных формах учебного процесса;
- разгрузка преподавателя от трудоемких операций, не требующих творческих действий;
- интенсификация учебного процесса;
- возможность самостоятельного обучения;
- возможность сбора и анализа статистики учебного процесса;
- всесторонний контроль учебного процесса;
- надежность функционирования.

Влияние электронного практикума процесс обучения производится на основе определенных показателей (критериев) обучения, путем применения качественных и количественных измерителей.

Можно выделить следующую совокупность показателей эффективности, с помощью которых возможно оценить влияние электронного практикума на качество формирования умений в области защиты персональных данных в сети Интернет:

− сокращение времени обучения за счет применения индивидуального обучения, соответствующих особенностям восприятия информации студентами;

− сокращение трудоемкости создания контрольных вопросов;

− сокращение времени поиска студентами необходимой при обучении информации;

− повышение качества усвоения учебного материала путем дублирования каналов восприятия учебной информации;

− повышение качества подготовки студентов за счет оптимизации индивидуальных образовательных траекторий, оказание индивидуальной помощи преподавателями при групповом обучении;

− повышение эффективности контроля за счет использования единых критериев оценки знаний и умений всех студентов, за счет учета затрат времени ответа, объема контролируемых знаний и других факторов;

− повышение качества контроля за счет адаптации электронного практикума к индивидуальным особенностям студентов путем введения обратной связи, определяющей стратегию контроля умений.

Существуют различные методики оценки эффективности применения электронных средств обучения.

Так, для оценки эффективности функционирования электронных средств обучения используется, например, критерий непосредственной экономической эффективности, который определяется как отношение затрат на обучение одного человека с помощью электронного средства обучения к

затратам на его обучение с использованием только традиционных методов обучения.

Сокращение времени обучения при обучении с использованием электронного практикума характеризуется коэффициентом:

$$К_{об} = \frac{T_1}{T_0} = \frac{N_0 \sum_{i=1}^{N_1} \sum_{j=1}^{n} t_{1ij}}{N_1 \sum_{j=1}^{N_1} \sum_{i=1}^{n} t_{0ij}}, \quad (5)$$

где T_1/T_0 - среднее время выполнения видов учебной деятельности при новом и обычном методах обучения;

N_i / N_0 - количество обучающихся с помощью электронного практикума и обычным методом;

n - число видов учебной деятельности, проведение которых автоматизировано;

t_{1ij}/t_{0ij} - время выполнения i-м студентом j-го вида учебной деятельности при использовании электронного практикума и традиционным методом соответственно.

Качество подготовки студентов колледжа также может быть оценено коэффициентом:

$$K_k = \frac{A_1}{A_0} = \frac{N_0 \sum_{i=1}^{N_1} \sum_{j=1}^{m} X_{1ij}}{N_1 \sum_{i=1}^{N_0} \sum_{j=1}^{n} X_{0ij}}, \quad (6)$$

где A_1/A_0 - качество подготовки педагога, обучающегося соответственно новым и традиционным методом обучения;

m - число оцениваемых эффектов выполнения j-ой работы i-ым специалистом;

X_{1ij} /X_{0ij} - величины, характеризующие выполнение i-ым студентом, обучавшимся с использованием электронного практикума и традиционным методом соответственно j-го вида работы за период t лет после окончания обучения.

Для оценки педагогических возможностей электронного практикума может быть рассчитан критерий дидактической целесообразности применения ЭВМ:

$$К = \frac{Э_В}{Э_Т}, \quad (7)$$

где $Э_Т$ - требуемый эффект;

$Э_В$ - возможный эффект.

Для расчета $Э_т$ и $Э_в$ функции электронного практикума расчленяются на элементы, выполнению которых можно поставить в соответствие однозначное «ДА» или «НЕТ».

Для сравнения различных электронных средств обучения и оценки эффективности использования вычислительной техники применяется критерий использования электронного средства обучения:

$$К_и = \frac{\sum_{i=1}^{s} a_i t_i}{\sum_{i=1}^{s} t_i}, \quad (8)$$

где t_i - время, затраченное на работу i-го вида при обучении;

s - число работ, автоматизированных с помощью ЭВМ;

a_i - коэффициент, учитывающий степень использования ЭВМ в i-том виде обучения $(0< a_i< 1)$.

Существует также еще целый ряд методик, позволяющих оценить качество учебного процесса и эффективность применения электронных средств обучения, в частности электронного практикума. Для разрабатываемого электронного практикума предлагается в качестве критерия эффективности выбрать коэффициент сокращения времени обучения (5), представляющий непосредственную экономическую эффективность электронного практикума и характеризующий повышение качества подготовки студентов колледжа за счет непосредственной экономической эффективности электронного практикума.

2.2 Описание среды разработки и структура электронного практикума «Защита персональных данных в сети Интернет»

В рамках магистерской диссертации было принято решение разработать электронный практикум, включающий практические задания, упражнения, кейс-задачи для формирования умений по защите персональных данных в сети Интернет для студентов колледжа.

Учитывая возможности, имеющегося в образовательной организации оборудования и программного обеспечения, необходимо создать современный программный продукт, избегая таких недостатков существующих коммерческих предложений, как высокая стоимость внедрения и сопровождения и слабая ориентированность на пользователя с разной профессиональной подготовкой. Также необходимо уделить особое внимание надежности приложения и простоте его интерфейса.

Сейчас на рынке программного обеспечения появился достаточно большой выбор средств создания обучающих систем.

Для создания электронного практикума можно использовать инструменты, встроенные в системы дистанционного обучения или специальное программное обеспечение. С помощью встроенных инструментов любой может сделать простой практикум, содержащий текст, видео, тесты. Используя специализированное программное обеспечение, получаются более сложные и интересные продукты, но и разработчик должен иметь определенные навыки работы [**Error! Reference source not found.**].

Чтобы начать разрабатывать электронный практикум при помощи онлайн-системы дистанционного обучения, не требуется наличие каких-то особенных знаний, не нужно знать языки программирования.

На текущий момент в мире существует множество систем дистанционного обучения. Для того, чтобы из множества систем выбрать наиболее подходящую была создана сравнительная таблица (таб. 5).

Таблица 5 – Сравнение систем дистанционного обучения для разработки электронного практикума

№ п/п	Наименование системы	Язык системы	Ценовая политика системы	Инструменты, используемые при разработке электронного курса
1.	Moodle	English Deutsch Español Français Italiano Português	Есть 5 пакетов: «Начинающий» $120 USD / год; «Мини» $220 USD / год; «Маленький» $400 USD / год; «Средний» $890 USD / год; «Большой» $1,580 USD/год. Есть пробный бесплатный период на 45 дней.	Возможность следить за прогрессом студентов. Поддержка мультимедиа. Возможность разрабатывать курсы, адаптированные под мобильные устройства, возможность интегрирования дополнений со сторонних ресурсов. Есть интеграция с платежной системой PayPal, которая делает простым процесс оформления заказов и оплаты.
2.	iSpring Learn	Русский	Тарифы отличаются друг от друга количеством пользователей 1. «50 пользователей» 56 000 ₽/ год; 2. «100 пользователей» 98 000 ₽/ год; 3. «200 пользователей» 174 000 ₽/ год; 4. «300 пользователей» 254 000 ₽/ год; Бесплатная 14-дневная пробная версия.	Мобильная версия. Детальная статистика. В платформу интегрирован профессиональный сервис для видеоконференций и вебинаров Zoom. Загружайте в iSpring Learn видеоуроки (FLV, MP4), Flash-ролики (SWF), аудиозаписи (MP3, WAV) или документы PDF, DOC(X), XLS, PPT-презентации. Возможность загружать в систему SCORM-пакеты, созданные в iSpring или сторонних программах разработки.

Продолжение таблицы 5

4.	Stepik	Русский	«Basic» – 0 рублей. «Pro» - 2900 ₽ за 1 PRO-курс в месяц. «Enterprise» - от 500 000 ₽/ год. «Pay-as-you-earn» - комиссия от 12% с платежа	Онлайн-редактор курса. Создание практических заданий с разным уровнем сложности: от тестов до свободных ответов. Возможность вставки видеофайлов. Возможность обратной связи. Выдача сертификатов (на платных тарифах). Возможность создания как открытых, так и приватных курсов

Исходя из данных, приведенных в таблице, было принято решение взять за основу для разработки электронного практикума онлайн-платформу iSpring Learn.

Для работы с платформой необходимо зарегистрировать учётную запись, а также выбрать тариф, от которого будут зависеть возможности по созданию и использованию электронного практикума. Тарифы и возможности приведены на таблице 6.

Изучив возможности платформы, было принято решение разрабатывать на бесплатном тарифе. На данном тарифе доступны автоматическая проверка решений, общение с обучающимися. Число курсов и число обучающихся не ограничивается.

Электронный практикум «Защита персональных данных в сети Интернет» воплощен с использованием инструментов образовательной платформы iSpring Learn.

Задачи электронного практикума «Защита персональных данных в сети Интернет»:

1. Приобретение теоретических знаний в области информационной безопасности.

2. Становление умения совершать выбор среди разнообразия технологий для защиты персональных данных в сети Интернет.

3. Усвоение знаний по сохранению информационной безопасности личности, а также сегментов образовательной организации.

Электронный практикум «Защита персональных данных в сети Интернет» рассчитан на обучающихся образовательных учреждений, не являющихся специалистами в области защиты информации.

В результате работы с практикумом обучающийся должен знать:

1. Законодательство в области информационной безопасности. Правовые основы организации защиты персональных данных.

2. Источники и классификацию угроз информационной безопасности.

3. Основные методы защиты информации.

В результате прохождения практикума обучающийся должен уметь:

1. Применять правовые, организационные и технические средства защиты информации.

2. Уметь работать с персональными данными с обеспечением защиты информации.

3. Организовывать безопасную работу в сети Интернет, безопасную отправку почтовых сообщений в глобальной сети.

4. Распознавать источники угроз информационной безопасности.

По освоению электронного практикума формируются следующие компетенции:

1. Способность справляться со стандартными задачами в профессиональной деятельности, используя информационно-коммуникационные технологии и учитывая основные правила по информационной безопасности.

2. Способность осознавать сущность и ценность информации в развитии информационного общества, понимать риски и угрозы, возникающие в этом процессе, блюсти основные правила информационной безопасности.

Структура электронного практикума разработана исходя из логики учебного процесса, отраженной в пошаговом усвоении учебного материала.

Для разработки электронного практикума была выбрана онлайн-платформа iSpring Learn.

iSpring Learn – российская образовательная интернет-платформа дистанционного обучения, выступающая в качестве конструктора бесплатных открытых онлайн-курсов и учебных единиц. Дает возможность зарегистрированному пользователю разрабатывать интерактивные обучающие занятия и онлайн-курсы, используя медиа, тексты и различные задачи. В платформу интегрирована автоматическая проверка решений обучающегося и качественная обратная связь [32].

Онлайн-сервис iSpring Learn (бывш. iSpring Online, рус. АйСпринг Лёрн) от компании Ричмедиа предназначен для управления обучением. Система обладает широким функционалом, является кросплатформенной, разворачивается как в облаке разработчика, так и на серверах клиента [35].

Программный продукт iSpring Learn позволяет планировать все имеющиеся учебные активности: онлайн-курсы, мастер-классы. Сервис собирает обширную статистистическую информацию и поддерживает отслеживание успеваемости обучающихся, так что информация о посещаемости становится доступна в отчётах и аналитических интерфейсах системы.

Интерфейс платформы полностью русскоязычный, достаточно дружелюбный и интуитивно понятный. Регистрация на платформе бесплатная.

Этапы создания электронного практикума.

1. Регистрация на платформе.
2. Формирование контента электронного практикума.

2.1. Подбор, редактирование теоретической части.

2.2. Подбор, составление практической части.

2.3. Подбор, редактирование и составление ссылок на дополнительные материалы.

3. Разработка структуры электронного практикума.

4. Разработка электронного практикума на платформе.

4.1. Создание практикума.

5. Создание тем, редактирование содержания.

6. Наполнение теоретической и практической частями.

Опишем основные элементы пользовательского интерфейса электронного практикума.

При запуске браузера, переходим на платформу iSpring Learn. Для прохождения и создания курсов необходима регистрация (рис. 2).

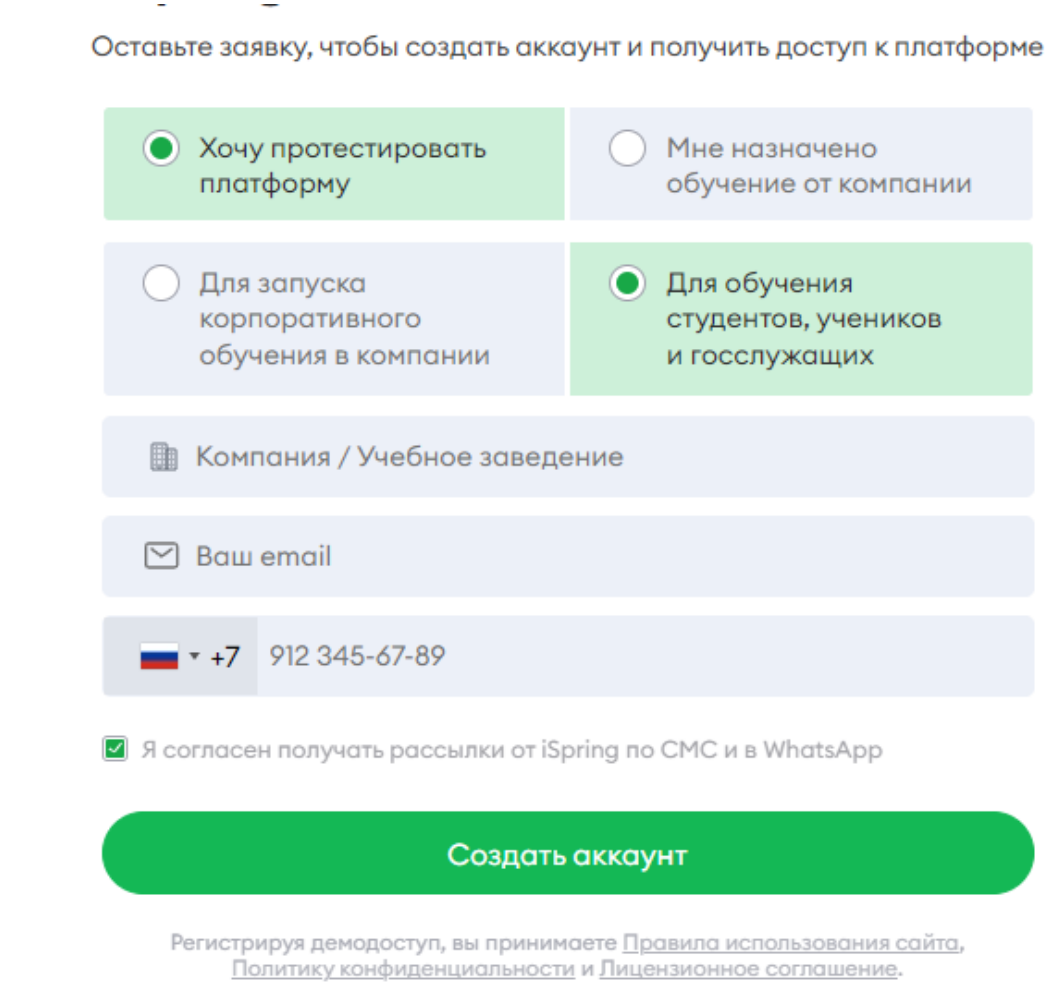

Рисунок 2 – Форма для регистрации на платформе iSpring Learn

После регистрации необходимо перейти на курс, используя прямую ссылку от преподавателя.

С левой стороны страницы находится навигационное меню, где можно ознакомиться с последовательностью тем (рис. 3).

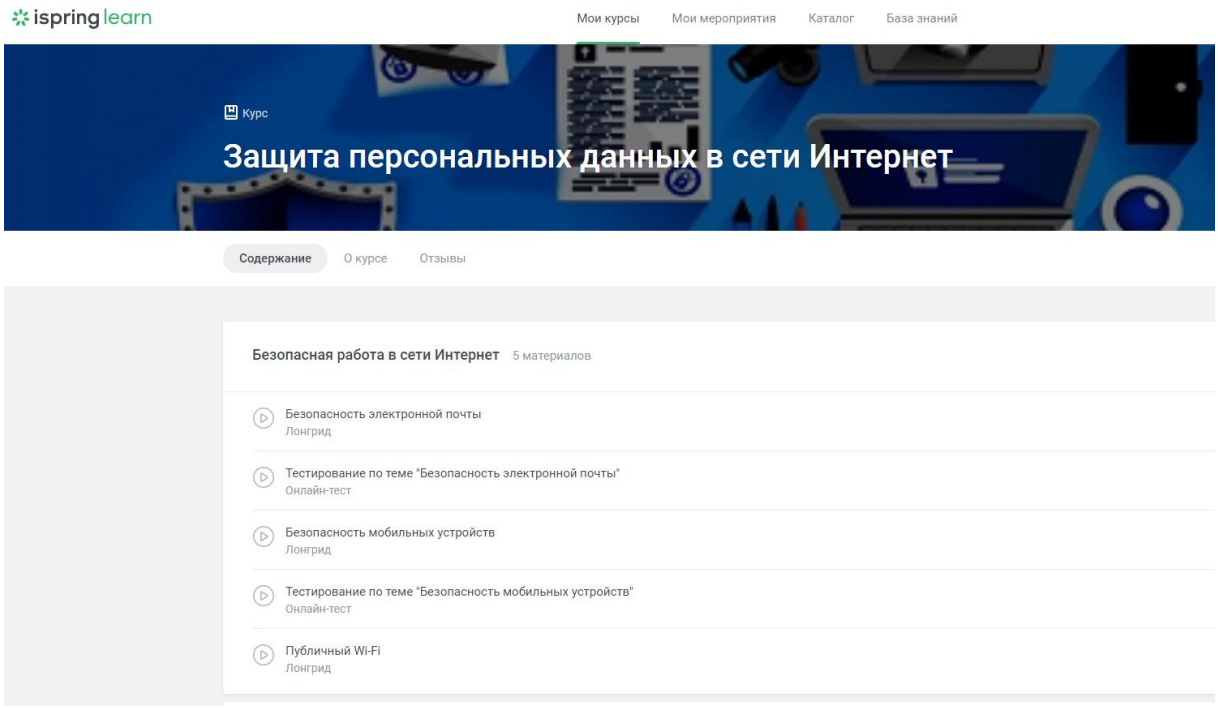

Рисунок 3 – Пользовательский интерфейс практикума «Защита персональных данных в сети Интернет» на платформе iSpring Learn

Первый раздел включает в себя теоретический материал (рис. 4) и тестовые задания (рис. 5).

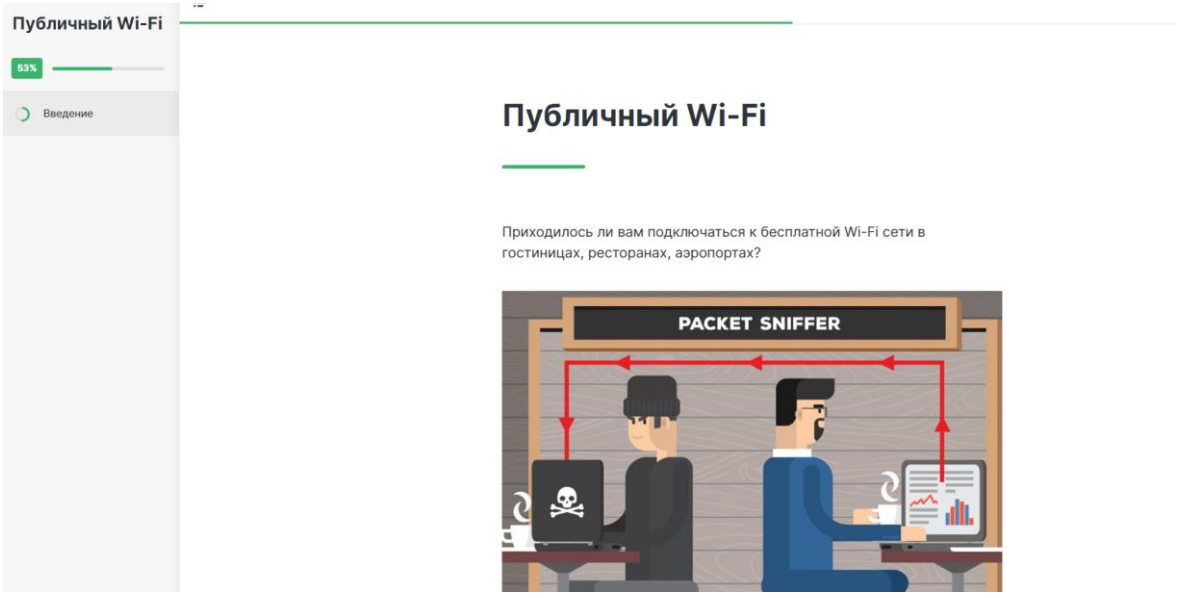

Рисунок 4 – Тема «Публичный Wi-Fi»

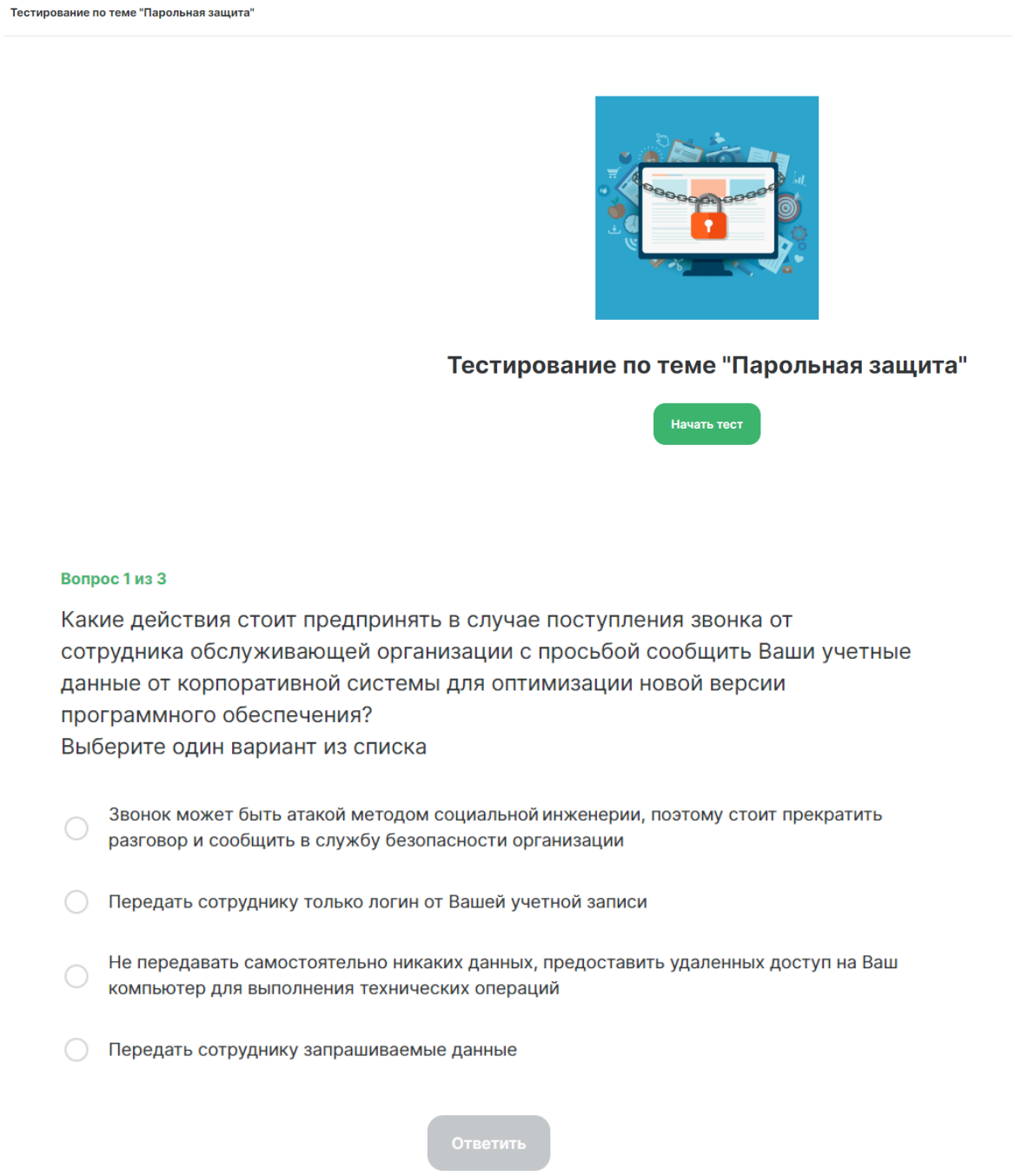

Рисунок 5 – Пример тестирования по теме «Парольная защита»

Второй раздел «Практикум» (рис. 6) включает в себя практические задачи, тестовые вопросы (рис. 7).

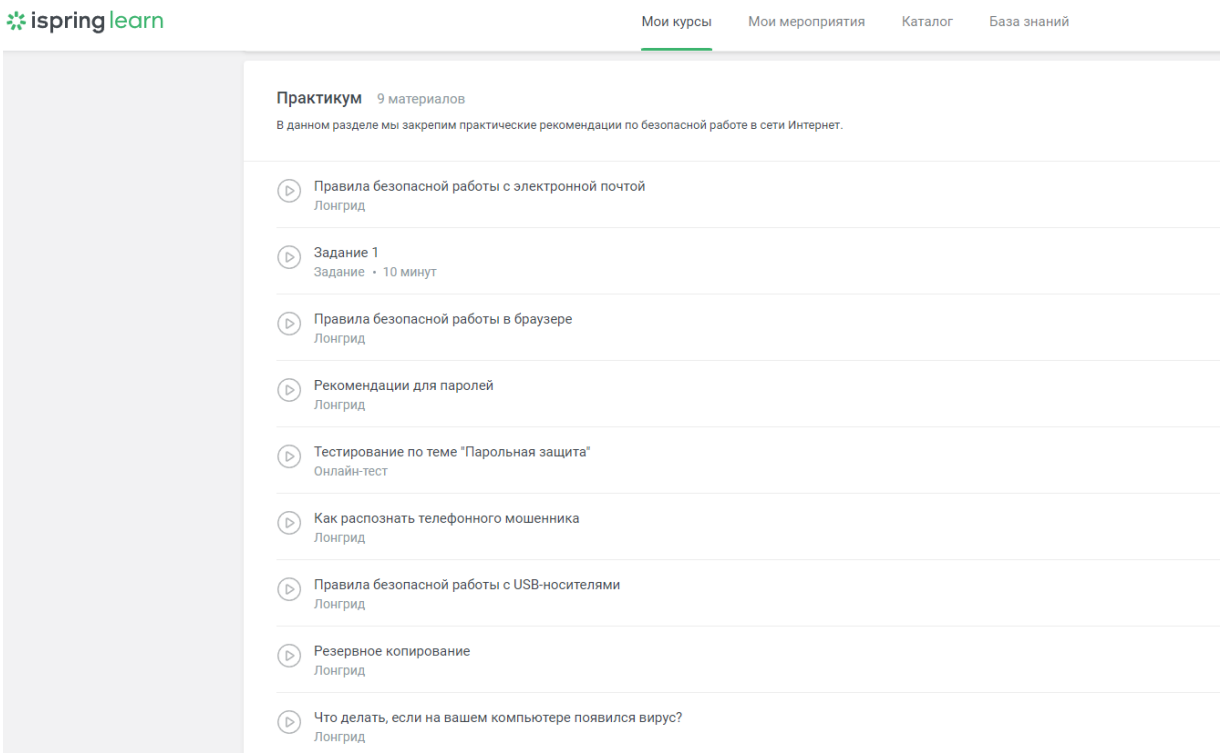

Рисунок 6 – Раздел «Практикум»

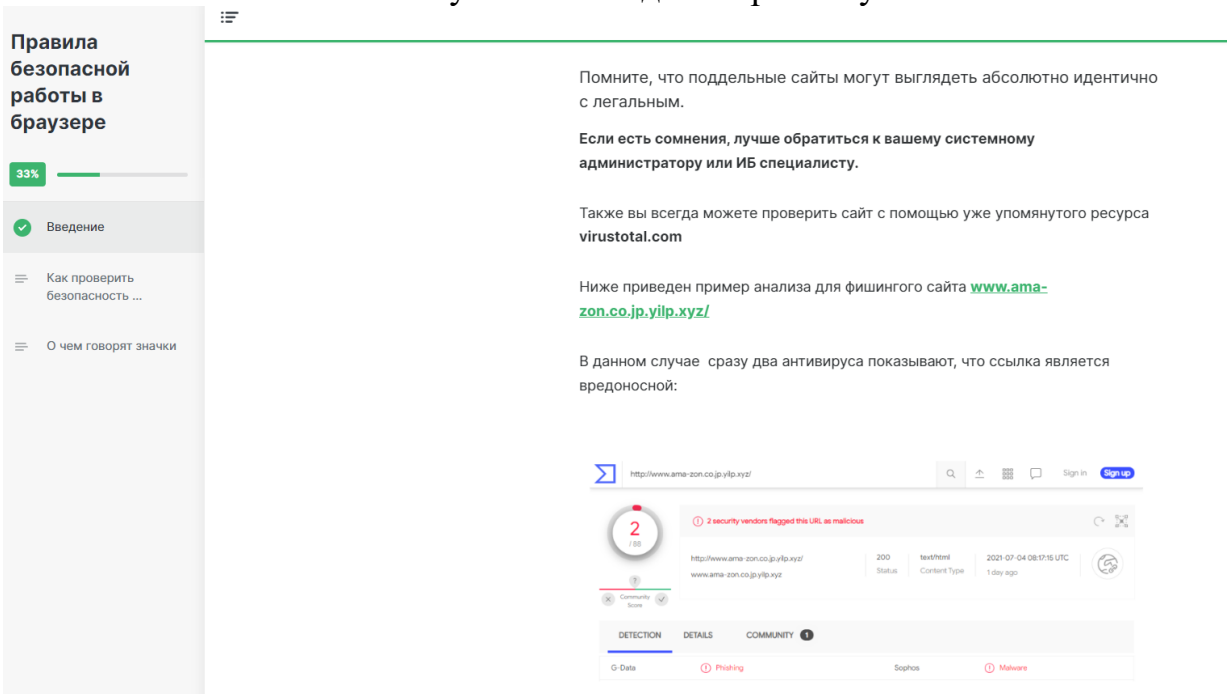

Рисунок 7 – Практическая работа по теме «Правила безопасной работы в браузере» на платформе iSpring Learn

Приведем примеры заданий.

Задание 1. Вы — сотрудник бухгалтерии и работаете с системами дистанционного банковского обслуживания. Вам на корпоративную почту поступает срочное сообщение от известного Вам банка, в котором содержится информация о том, что на счет компании поступил возврат кассовых издержек (рис. 8). Что нужно сделать в данном случае?

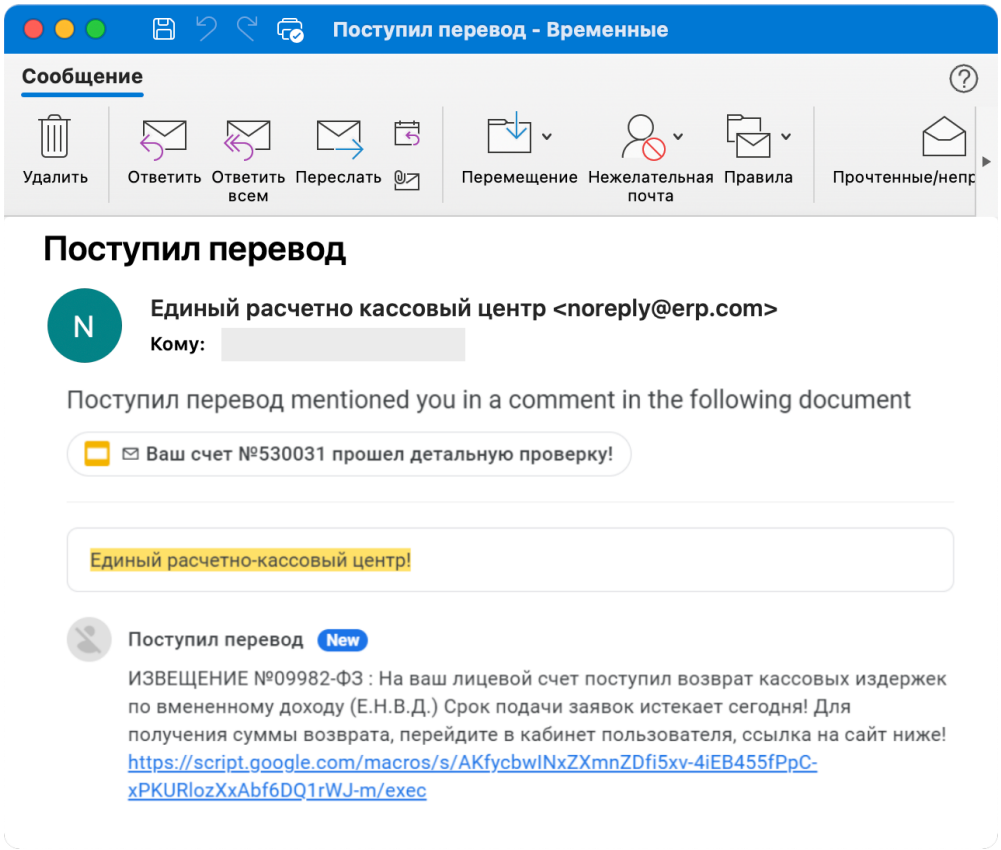

Рисунок 8 – Электронное письмо

Задание 2. Вы хотите купить квартиру, и недавно подали заявку на ипотеку в три банка. Спустя два дня получаете следующее смс с предложением перейти по ссылке (рис. 9). Как поступите?

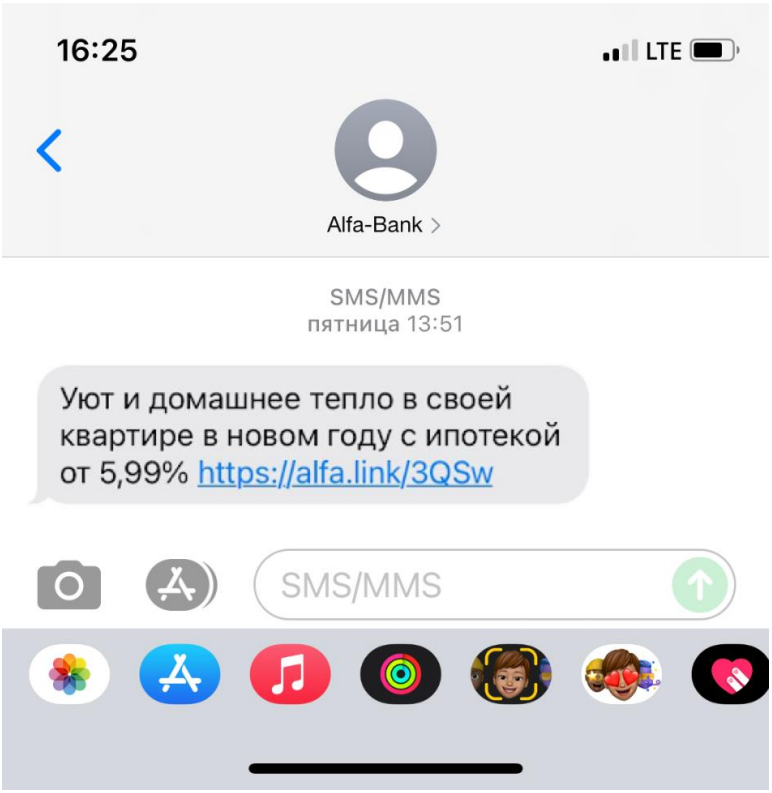

Рисунок 9 – Пример SMS

Следующая задача исследования применение в учебном процессе ГБПОУ «Южно-Уральский государственный технический колледж» разработанный электронный практикум по теме «Защита персональных данных в сети Интернет».

2.3 Апробация электронного практикума как средства формирования умений по защите персональных данных в сети Интернет студентов колледжа на базе ГБПОУ «Южно-Уральский государственный технический колледж»

В целях выявления эффективности применения электронного практикума по теме «Защита персональных данных в сети Интернет» была проведена экспериментальная проверка на базе ГБПОУ «Южно-Уральский государственный технический колледж», располагающийся по адресу: г. Челябинск ул. Гагарина, 7.

В колледже реализуются образовательные программы среднего профессионального образования, основные программы профессионального

обучения, дополнительные общеобразовательные и профессиональные программы, услуги по содержанию и воспитанию обучающихся в общежитии, организация и проведение мероприятий в сфере образования и науки.

Основные задачи колледжа определяются в соответствии с нормативно-правовыми актами Российской Федерации и реализуются в соответствии с Уставом колледжа [36]:

– удовлетворение потребностей граждан в получении профессионального образования в избранной профессиональной деятельности, в интеллектуальном, культурном, физическом и нравственном развитии;

– удовлетворение потребностей общества в профессионально подготовленных специалистах, создании новых рабочих мест;

– профессиональная переподготовка и повышение квалификации специалистов и рабочих;

– распространение знаний среди населения, повышение его общеобразовательного и культурного уровня, в том числе путем оказания платных образовательных услуг.

В своей образовательной деятельности колледж использует наиболее эффективные технологии обучения и воспитательные системы.

Доступ педагогических работников к информационно-телекоммуникационной сети Интернет в колледже осуществляется с персональных компьютеров (ноутбуков и т.п.), подключенных к сети Интернет, без ограничения времени и потребленного трафика.

Для доступа к информационно-телекоммуникационным сетям в колледже педагогическому работнику предоставляются идентификационные данные (логин и пароль). Предоставление доступа осуществляется системным администратором колледжа.

Доступ к электронным базам данных осуществляется на условиях, указанных в договорах, заключенных колледжем с правообладателем электронных ресурсов (внешние базы данных).

Информация об образовательных, методических, научных, нормативных и других электронных ресурсах, доступных к пользованию, размещена на сайте колледжа.

В ходе учебного процесса применяются дистанционные образовательные технологии с использованием таких систем как e.lanbook.ru, moodle, dom.sustec.ru [36].

Для осуществления дистанционной образовательной деятельности, размещения информации о предстоящих и прошедших мероприятиях и информирования студентов об актуальных событиях у ГБПОУ «Южно-Уральский государственный технический колледж» имеется собственный сайт (режим доступа: https://sustec.ru), отвечающий всем требованиям к подобным ресурсам образовательных организаций [36].

Для достижения целей обучения студентов по защите персональных данных в сети Интернет предлагается использовать электронный практикум, который включает:

– рабочую программу дисциплины «Информационная безопасность», объединяющие инвариантную часть и вариативные компоненты для различных специальностей;

– электронный практикум; оценочный материал для автоматизированной системы оценки и контроля знаний по информационной безопасности.

В процессе обучения необходимо развивать у студентов способность к самоуправлению, саморегуляции и самокоррекции, чувство ответственности за свою судьбу, преодолевать пассивность, стремиться к целенаправленному и упорному самосовершенствованию.

В соответствии с целями педагогического взаимодействия развивается учебно-познавательная деятельность обучаемых, направленная

на повышение уровня информационной культуры и обученности информационной безопасности и реализующая образовательный потенциал в многоуровневой системе информационной подготовки.

На занятиях по информационной безопасности следует исходить из основных принципов интенсификации и активизации обучения и использовать такие приемы организации сенсорного пространства, как: интенсификация процесса восприятия при обучении; оптимальное использование резервов памяти; активизация работы психологического механизма мышления; использование наглядности в формировании психического образа; использование суггестивных средств для интенсификации обучения; применение альтернативных образовательных технологий.

Электронный практикум по теме «Защита персональных данных в сети Интернет» может рассматриваться как совокупность средств обучения, используемых на различных этапах учебно-познавательного процесса и обеспечивающих единство педагогического воздействия.

Целями разработки такого электронного практикума являются:

- совершенствование педагогического мастерства;
- оптимизация подготовки и проведения занятий по информационной безопасности;
- обеспечение преемственности положительного опыта;
- интенсификация учебно-воспитательного процесса;
- развитие познавательной активности студентов системой дифференцированных заданий с учетом их индивидуальных способностей;
- обеспечение дидактического единства усвоения системы знаний и развитие творческой познавательной деятельности студентов в области защиты персональных данных в сети Интернет.

Электронный практикум обеспечивает планирование учебного материала, что способствует вариативности его построения. Учебные модули, как самостоятельные блоки учебной информации в области

защиты персональных данных в сети Интернет, включают в себя цели и учебную задачу, методические рекомендации, ориентировочную основу действий и средства контроля (самоконтроля) успешности учебной деятельности.

Экспериментальная проверка применения является одним из методов педагогического исследования.

В экспериментальной работе были задействованы студенты второго курса группы ПР-263/б (26 чел.), обучающиеся специальности «Информационные системы и программирование», поделенные на две подгруппы по 13 человек.

В процессе педагогической практики было проведено 3 практических занятий по следующим темам:

1. Анализ рисков информационной безопасности.

2. Построение концепции информационной безопасности предприятия.

3. Персональные данные и личная информация. Защита персональных данных в сети Интернет.

Последнее занятие проводилось в форме контрольной практической работы.

На первом этапе происходило выявление исходного уровня сформированности специальных умений студентов по дисциплине «Информационная безопасность». На данном этапе применялись следующие методы для определения уровня специальных умений студентов по теме:

– наблюдение;

– анализ выполнения практических работ по дисциплине в начальный период ее изучения до применения электронного практикума.

В методике профессионального обучения выделяют следующие уровни овладения обучающимися специальными умениями и навыками по дисциплине:

0 уровень - обучающиеся совершенно не владеют данным действием (нет умения).

1 уровень - обучающиеся знакомы с характером данного действия, умеют выполнять его лишь при достаточной помощи преподавателя;

2 уровень - обучающиеся умеют выполнять данное действие самостоятельно, но лишь по образцу и подражая действиям сверстников;

3 уровень - обучающиеся умеют достаточно свободно выполнять действия, осознавая каждый шаг;

4 уровень - обучающиеся автоматизировано, свернуто и безошибочно выполняют действия (навык).

При определении уровня сформированности умений можно использовать подход количественной обработки результатов диагностики, который позволяет в отношении степени проявления каждого уровня определить количественный показатель. В нашем исследовании ввели следующие количественные показатели:

1) баллом «0» отмечали низкий уровень сформированности умений и навыков (НУ);

2) баллом «1» обозначали средний уровень (СУ);

3) баллом «2» обозначали оптимальный (высокий) уровень (ВУ).

Для определения начального уровня сформированности умений были взяты результаты практической контрольной работы группы ПР-263/б по предыдущей теме, которая изучалась под руководством ведущего педагога. Результаты исходного уровня сформированности умений представлены в таблице 6.

Таблица 6 − Результаты начального уровня сформированности умений у студентов до применения электронного практикума

Группы	Уровень сформированности умений студентов по результатам практической контрольной работы				
	Количество студентов	Отлично (%)	Хорошо (%)	Удов-но (%)	Неудов-но (%)
Контрольная	13	23%	38,5%	38,5%	-
Экспериментальная	13	23%	46,2%	30,8%	-

Обобщенные результаты практической контрольной работы студентов в опытной и контрольной подгруппах представлены на рисунке 10.

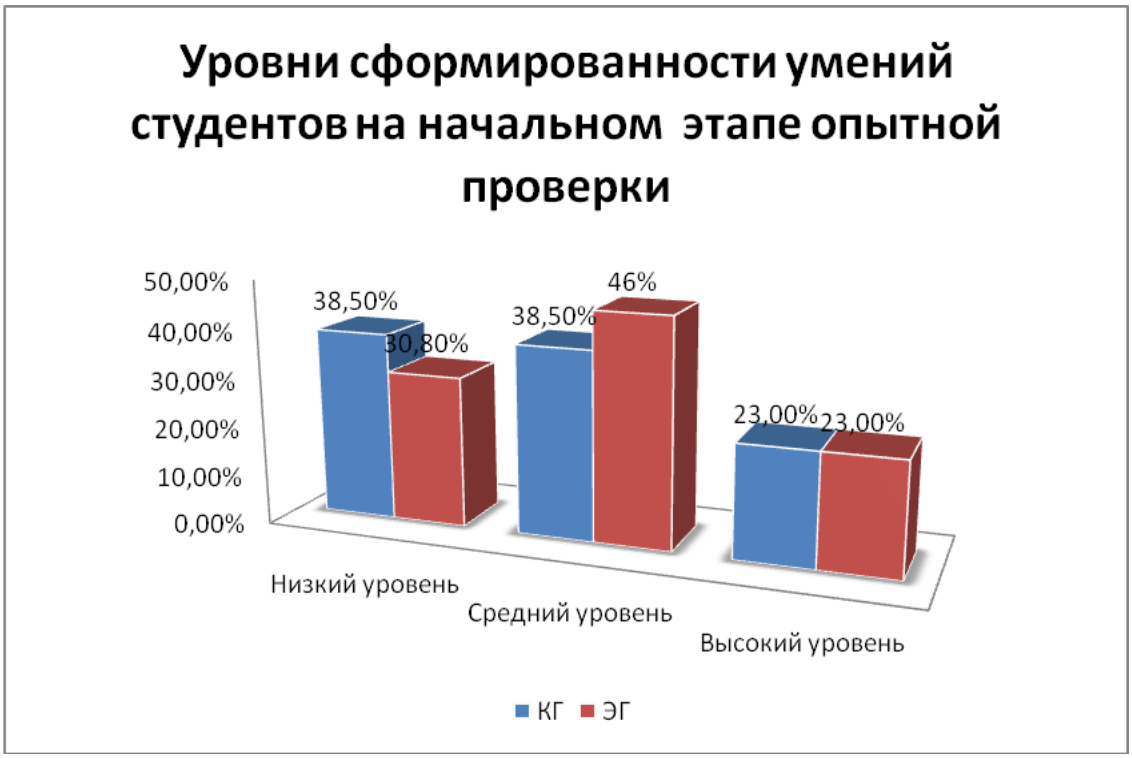

Рисунок 10 – Результаты исследования начального уровня сформированности специальных умений студентов

Таким образом, уровень первоначальных умений обучающихся в подгруппах группах по данной теме практически одинаковый, что позволило проводить дальнейшее исследование.

Целью обучающего этапа экспериментальной проверки является внедрение электронного практикума по дисциплине «Информационная безопасность» в ходе проведения уже педагогической практики и определения его влияния на уровень сформированности специальных умений.

Задачи этапа:

1. Применить разработанный электронный практикум по теме «защиты персональных данных в сети Интернет» в процессе проведения занятий по дисциплине «Информационная безопасность».

2. Определить влияние применения электронного практикума по теме «Защита персональных данных в сети Интернет» на результаты обучения, в качестве которых рассматривали уровень сформированности специальных умений обучающихся.

Далее были уточнены условия проведения экспериментальной проверки: изменяющиеся и постоянные.

В качестве изменяющихся условий экспериментальной проверки для экспериментальной группы были предложены:

− применение в качестве средства обучения в условиях самостоятельной работы: дополнительных практических заданий посредством электронного практикума;

− выдача заданий с подробными методическими указаниями по их выполнению при выполнении лабораторных работ посредством электронного практикума.

В качестве постоянных условий опытной проверки для контрольной и экспериментальной групп выступают следующие:

− постановка одинаковых для обеих групп дидактических задач, решаемых в ходе занятий;

− одинаковое время длительности экспериментального обучения;

− одинаковые формы и виды входного и итогового контроля;

− один и тот же педагог в контрольной и экспериментальной группах.

Далее были проведены занятия, причем в экспериментальной группе они проводились с использованием разработанной электронного практикума по теме «Защита персональных данных в сети Интернет» в рамках занятий по дисциплине «Информационная безопасность», а в контрольной группе применялась только тестирующая программа.

Цель контрольного этапа – анализ эффективности внедрения электронного практикума по теме «Защита персональных данных в сети Интернет».

Контрольный этап экспериментальной проверки включает в себя итоговый контроль, который направлен на проверку конечного уровня сформированности умений, полученных в ходе аудиторной самостоятельной работы на основе электронного практикума по теме «Защита персональных данных в сети Интернет».

Итоговый контроль проводился на основе практической контрольной работы по решению практических задач и ситуаций, в которых требовалось применить практические умения, приобретенные в ходе работы с электронным практикумом. Результаты итогового контроля показаны в таблице 7.

Таблица 7 − Результаты итогового контроля результатов обучения студентов

Группы	Распределение обучающихся КГ и ОГ по результатам итогового контроля				
	Количество учащихся	Отлично (%)	Хорошо (%)	Удов-но (%)	Неудовлетворительно (%)
Контрольная	13	23%	46,2%	30,8%	-
Экспериментальная	13	38,5%	46,1%	15,4%	-

Экспериментальная проверка по применению электронного практикума в процессе проведения практических занятий показала следующее:

1. В экспериментальной группе все студенты смогли выполнить требуемые практические задания и ситуации.

2. Многие студенты экспериментальной группы, благодаря самостоятельной работе на основе электронного практикума, проявили умения и навыки на более высоком уровне по изучаемой теме.

Результаты приведены на рисунке 11.

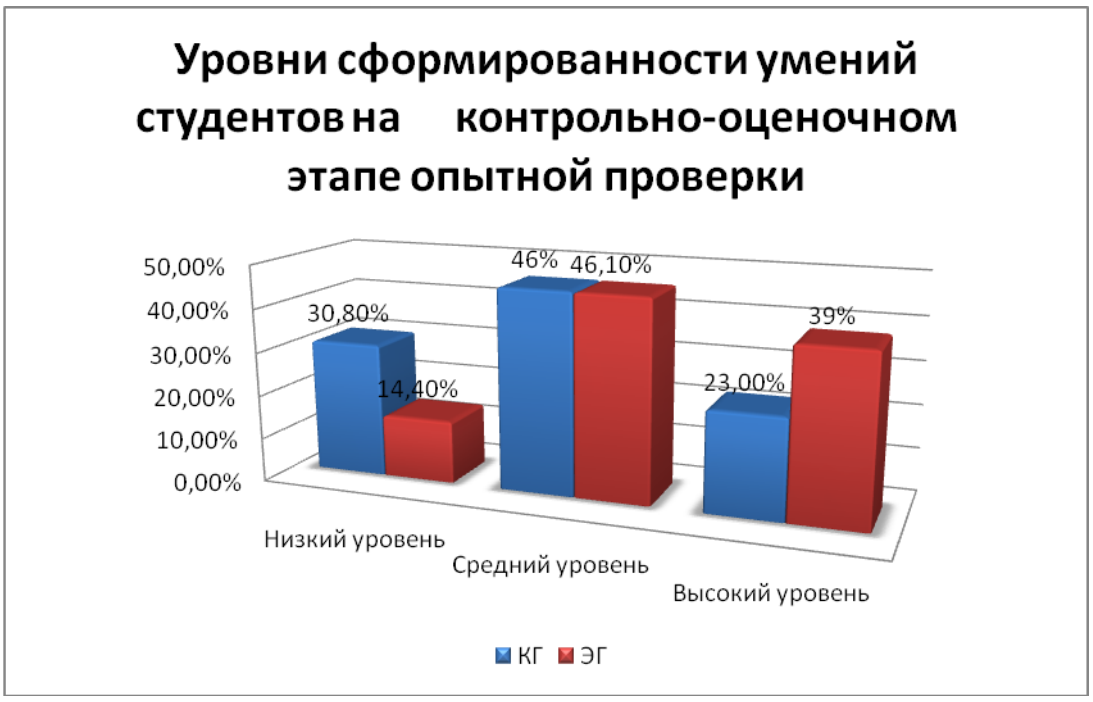

Рисунок 11 – Уровни сформированности умений студентов на контрольно-оценочном этапе экспериментальной проверки

Контрольный этап экспериментальной проверки показал, что обучение с использованием разработанного и внедренного в педагогический процесс электронного практикума является, с точки зрения дидактики, результативным.

В итоге снизились показатели низкого уровня в опытной подгруппе на 15%, а в контрольной группе на 7,7%. Средние показатели в экспериментальной группе несколько увеличились по сравнению с начальным этапом и составили 8%, в контрольные средние показатели остались на прежнем уровне. И, наконец, высокие показатели в экспериментальной группе, по сравнению с начальным этапом увеличились на 15%. Высокие показатели контрольной группы остались на прежнем уровне.

В результате проведенной экспериментальной проверки можно сделать следующие выводы:

1. Проведенная экспериментальная проверка показала положительные тенденции в уровне сформированности умений студентов

по теме «Защита персональных данных в сети Интернет» с применением электронного практикума.

2. Эффективность электронного практикума достигнута благодаря соблюдению методологических и методических требований к его проектированию как дидактического средства.

3. Результаты итогового контроля студентов показали, что в экспериментальной группе повысился уровень сформированности умений.

Таким образом, можно сказать, что применение разработанного электронного практикума по теме «Защита персональных данных в сети Интернет» способствует повышению эффективности и качества учебного процесса в колледже при изучении дисциплины «Информационная безопасность».

Согласно результатам проведения экспериментальной проверки применения электронного практикума «Защита персональных данных в сети Интернет», можно сделать вывод, что эффективность его использования при изучении дисциплины «Информационная безопасность» повысилась. Это обусловлено тем, что в практике подготовки будущих специалистов по направлению «Информационные системы и программирование» был использован разработанный электронный практикум.

Выводы по Главе II

Во второй главе магистерской диссертации был разработан электронный практикум по теме «Защита персональных данных в сети Интернет» в рамках изучения дисциплины «Информационная безопасность».

Электронный практикум «Защита персональных данных в сети Интернет» рассчитан на обучающихся образовательных учреждений, не являющихся специалистами в области защиты информации. Для

разработки электронного практикума была выбрана онлайн-платформа iSpring Learn.

Электронный практикум по теме «Защита персональных данных в сети Интернет» включает в себя теоретический материал, практические задачи и тестовые задания.

Экспериментальная проверка эффективности применения разработанного электронного практикума по теме «Защита персональных данных в сети Интернет» была проведена на базе колледжа ГБПОУ «ЮУрГТК».

В ходе проведения экспериментальной проверки были использованы практическая контрольная работа для определения начального уровня сформированности умений, и решение практических задач и ситуаций, в которых требовалось применить специальные умения, приобретенные в ходе работы с электронным практикумом.

Результаты проведения экспериментальной проверки применения разработанного электронного практикума по теме «Защита персональных данных в сети Интернет» свидетельствуют о его эффективности с точки зрения формирования умений по защите персональных данных в сети Интернет у студентов колледжа.

ЗАКЛЮЧЕНИЕ

Для решения в системе среднего профессионального образования педагогических проблем, связанных с обучением основам информационной безопасности и защиты персональных данных как инвариантной составляющей информационной подготовки, направленной на формирование умений по защите персональных данных в сети Интернет, требуется системный подход, реализующий методологические, организационные, содержательные, дидактические аспекты. Система подготовки в области информационной безопасности и защиты персональных данных в сети Интернет должна быть детерминирована по всем уровням образовательной деятельности, как общего, так и профессионального образования: среднего, высшего, послевузовского, дополнительного, и ориентирована на различные специальности и специализации.

Формирование умений в области информационной безопасности у студентов колледжа при преподавании специальных дисциплин является важной задачей, которая требует особого внимания и подхода.

Данное исследование решает проблему разработки теоретических и методологических основ профессиональной подготовки студентов колледжа, обладающих умениями по защите персональных данных в сети Интернет в условиях цифровизации общества и образования. Результаты проведенного исследования позволили сделать следующие общие выводы:

1. Проблема информационной безопасности представляет собой сложное социально-политическое явление, и ее разрешение во многом зависит от совершенствования системы образования в части формирования умений в области информационной безопасности студентов колледжа, в частности по защите персональных данных в сети Интернет.

2. Формирование умений является важной педагогической задачей. Формирование умений во многом зависит от тех условий, которые созданы

для обучения, организации процесса выполнения тренировочных задач и упражнений, индивидуальных особенностей (возможностей) обучающегося.

Формирование умений по защите персональных данных в сети Интернет может быть достигнуто через включение соответствующих тем в учебные планы и программы подготовки специалистов среднего звена, проведение практических занятий и проектов, а также использование специализированных учебных материалов и ресурсов. Студенты должны быть ознакомлены с основными понятиями и принципами информационной безопасности, такими как конфиденциальность, целостность и доступность данных. Они должны понимать, что персональные данные являются конфиденциальной информацией и требуют особой защиты. В сфере информационной безопасности постоянно появляются новые угрозы и технологии. Поэтому важно обеспечить регулярное обновление знаний и навыков студентов в этой области. Студенты должны освоить практические навыки по защите персональных данных в сети Интернет, различные угрозы безопасности информации, связанные с использованием сети Интернет, возможные последствия нарушения правил безопасности и понимать важность соблюдения этих правил.

Данные аспекты являются важными для формирования умений по защите персональных данных в сети Интернет у студентов колледжа при обучении специальных дисциплин. Это требует совместных усилий преподавателей, администрации колледжа и самих студентов, а также постоянного обновления и совершенствования образовательных программ и методик.

3. В целях повышения эффективности процесса подготовки студентов колледжа и применения инновационных технологий электронного обучения был разработан электронный практикум по теме «Защита персональных данных в сети Интернет» для формирования и оценивания умений по защите персональных данных в сети Интернет, с

помощью которого можно не только проводить обучение, но и оценивать степень сформированности умений с учетом влияющих на этот процесс факторов. Для разработки электронного практикума была выбрана онлайн-платформа iSpring Learn.

4. Результаты, полученные в ходе применения разработанного электронного практикума по теме «Защита персональных данных в сети Интернет» на базе колледжа ГБПОУ «ЮУрГТК» подтвердили предположение о том, что использование практикума активизирует познавательные силы и творческие возможности студентов, повышает мотивацию студентов применять умения в будущей профессиональной деятельности, способствует формированию умений в области информационной безопасности, в частности по защите персональных данных в сети Интернет.

Результаты исследования рекомендуется использовать в практической деятельности образовательных организаций среднего профессионального образования с целью их внедрения в процесс профессиональной подготовки. Понимание проблематики информационной безопасности подготавливаемыми в системе среднего профессионального образования специалистами может быть достигнуто образовательной деятельностью по нескольким взаимодополняющим направлениям: получением базового образования в области информационной безопасности в рамках существующих специальностей; прохождением профессиональной переподготовки или получением дополнительной квалификации; внедрением во все специальности, не относящиеся к группе специальностей «Информационная безопасность» отдельной одноименной дисциплины; совершенствованием информационной подготовки специалистов в области информационной безопасности за счет введения в соответствующие Федеральные государственные образовательные стандарты среднего профессионального образования дидактических единиц, объективно отражающих значимость

и научный уровень решения этой проблемы, создания и укрепления внутридисциплинарных связей дисциплин информационного цикла и междисциплинарных связей с дисциплинами других разделов.

Таким образом, цель работы достигнута, задачи выполнены, гипотеза нашего исследования подтвердилась.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Алтуфьева А.А. Методические основы обучения информационной безопасности на базе телекоммуникационных ресурсов сети Интернет. автореф. дисс. … канд. пед. наук: 13.00.02. / Алтуфьева Александра Андреевна. - Санкт-Петербург, 2008. – 19 с.

2. Баданов А.Г. Информационная безопасность образовательного учреждения. Использование компьютерных технологий и работа в сети Интернет / А. Г. Баданов. − URL: http://dostizenie.ucoz.ru/document/badanov-2010-old_variant.pdf (дата обращения: 08.09.2023).

3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных деятельности [Электронный ресурс]: [базовая модель ФСТЭК РФ от 15.02.2008 г.]. − URL: www.consultant.ru. (дата обращения: 20.10.2023).

4. Банк данных угроз безопасности информации [Электронный ресурс]. – URL: https://bdu.fstec.ru/threat-section (дата обращения: 20.11.2023).

5. Белов Е.Б. Образование в области информационной безопасности: принципы совершенствования подготовки кадров / Е.Б. Белов, В.П. Лось // Информация и связь. − 2012. − №2. −С. 94-96.

6. Белов Е.Б. Состояние, проблемы и развитие профессионального образования в области информационной безопасности / Е.Б. Белов // Безопасность информационных технологий. −2015. − №1. − С. 6-13.

7. Бим-Бад Б.М. Педагогический энциклопедический словарь. Москва: Большая Российская энциклопедия, 2012.

8. Богатырева Ю.И. Подготовка будущих педагогов к обеспечению информационной безопасности школьников: автореф. дисс. … докт. пед. наук: 13.00.08 / Богатырева Юлия Игоревна. – Тула, 2014. – 42 с.

9. Ганзенко А. Формирование умений в педагогике / А. Ганзенко. – URL: https://spravochnick.ru/pedagogika/formirovanie_umeniy_v_pedagogike/ (дата обращения: 20.11.2023.

10. Голембиовская О.М. Автоматизация мониторинга защищенности информационных систем персональных данных / О.М. Голембиовская // Развитие регионов, как фактор укрепления единства и целостности государства. Сборник научно- практических статей. – Рыбница: 2012. – № 2. – С.63-68.

11. Голембиовская О.М. Формализация критериев выбора состава средств защиты информационных систем на основе оценки показателей угроз и уязвимостей / О. М. Голембиовская, В. И. Аверченков, М. Ю. Рытов // Информация и безопасность. – Воронеж, № 4, 2019. – С. 31-37.

12. Горбатов В.С. Концепция развития межведомственной системы подготовки специалистов в области обеспечении информационной безопасности / В.С. Горбатов, А.А. Малюк, А.И. Толстой // Безопасность информационных технологий. − 2015. − №2. −С. 18-20.

13. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

14. ГОСТ Р ИСО/МЭК 14764-2002. Сопровождение программных средств.

15. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. - М: Стандартинформ, 2006. – URL: https://www.niisva.su/wp-content/uploads/2014/09/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_%D0%98%D0%A1%D0%9E-%D0%9C%D0%AD%D0%9A_17799-2005.pdf.

16. Государственный реестр сертифицированных средств защиты информации. – URL: https://reestr.fstec.ru/reg3 (дата обращения: 05.10.2023).

17. Деенков А.Н. Система подготовки в области информационной безопасности студентов колледжа / А. Н. Деенков // Фундаментальные научные исследования: теория и практика. Сборник научных трудов по материалам XXII Международной научно-практической конференции (г.-к. Анапа, 15 января 2024 г.). – Анапа: Изд-во «НИЦ ЭСП» в ЮФО, 2024. – С. 46-51.

18. Димов Е.Д. Методика обучения студентов вузов технологиям защиты информации в условиях фундаментализации образования: автореф. … канд. пед. Наук: 13.00.02. / Димов Евгений Дмитриевич. – М.: Типография ООО «Ай-клуб» (Печатный салон МДМ), 2013. - 25 с.

19. Доктрина информационной безопасности Российской Федерации (Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646). – URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html.

20. Дубровин О. В. Защита персональных данных в сети Интернет: пользовательское соглашение / О. В. Дубровин, И. Ю. Ковалева // Вестник ЮУрГУ. Серия: Право. − 2014. − №2. − URL: https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-v-seti-internet-polzovatelskoe-soglashenie (дата обращения: 17.11.2023).

21. Защита персональных данных на сайте в сети Интернет. − URL: https://it-jurist.ru/yuridicheskie-uslugi/zashchita-personalnykh-dannykh-na-sayte/ (дата обращения: 18.11.2023).

22. Коджаспирова Г.М. Словарь по педагогике / Г. М. Коджаспирова. − Москва: МарТ, 2013.

23. Кузнецова С.Л. Современное состояние теории методов обучения / С. Л. Кузнецова // Мир науки, культуры, образования. − 2011; № 4: 141-145.

24. Лачина Е. А. Проблемы защиты персональных данных в сети «Интернет» / Е. А. Лачина, И. А. Кузнецова, Е. В. Носова // Ученые записки. – 2021. – № 1(37). – С. 114-118.

25. Методы системного педагогического исследования. Учебное пособие. / Под ред. Проф. Н.В. Кузьминой - Ленинград, Изд-во ленинградского ун-та, 1980.- 68 с.

26. Новиков А. М. Процесс и методы формирования трудовых умений / А. М. Новиков. – М.: Высш. шк., 1986. – 288 с.

27. О персональных данных [Электронный ресурс]: [федеральный закон: от 27.07.2006 г. № 152-ФЗ, в ред. от 04.06.2014 г. № 152-ФЗ]. - Режим доступа: www.consultant.ru (дата обращения: 01.10.2023).

28. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: [федеральный закон: от 27.07.2006 г. №149-ФЗ, в ред. от 06.04.2011 г. № 149-ФЗ]. – Режим доступа: www.consultant.ru (дата обращения: 10.09. 2023).

29. Об образовании в Российской Федерации [Электронный ресурс]: [федеральный закон: от 29.12.2012 №273-ФЗ, в ред. от 17.02.2023 №26-ФЗ]. – Режим доступа: www.consultant.ru. Дата обращения: 10.05. 2022.

30. Об утверждении состава содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: [Приказ ФСТЭК России от 18 февраля 2013 г. № 21, в ред. от 14.05.2020 г. № 68]. – Режим доступа: https://fstec.ru/ (дата обращения: 20.10.2023).

31. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление 6 Правительства РФ от 01.11.2012 № 1119 // Собр. законодательства Рос. Федерации. – 2012. - № 45, ст. 6257/

32. Обзор СДО iSpring Learn: возможности и решаемые бизнес-задачи. − URL: https://lmslist.ru/sdo/obzor-ispring-online/ (дата обращения: 22.12.2023).

33. Общие эргономические требования к электронному практикуму и реализация их в работе. − URL: http://studopedia.org/7-141124.html (дата обращения: 18.11.2023).

34. Оладько В. С. Состав и структура дисциплины основы информационной безопасности / В. С. Оладько // Образование: прошлое, настоящее и будущее: материалы II Междунар. науч. конф. (г. Краснодар, февраль 2017 г.). − Краснодар: Новация, 2017. − С. 79-83. − URL https://moluch.ru/conf/ped/archive/211/11708/ (дата обращения: 02.12.2023).

35. Описание системы iSpring Learn. − URL: https://soware.ru/products/ispring-learn (дата обращения: 22.12.2023).

36. Официальный сайт ГБПОУ «Южно-Уральский государственный технический колледж». – URL: https://sustec.ru/ (дата обращения: 22.11.2023).

37. Памятка: Информационная безопасность в сети Интернет − URL: https://vokb1.ru/for-patients/pamyatka-informatsionnaya-bezopasnost-v-seti-internet/ (дата обращения: 18.11.2023).

38. Педагогика: учеб. пособие для студентов педагогических учебных заведений / В.А. Сластенин [и др.]. – М.: Школа-Пресс, 1997. – 512 с.

39. Полат Е.С. Проблема информационной безопасности в образовательных сетях рунет [Электрон. ресурс] / Е.С. Полат. − URL: http://www.ioso.ru/distant/library/publication/infobez.htm (дата обращения: 29.11.2023).

40. Поляков В. П. О системе обучения студентов основам информационной безопасности / В. П. Поляков // Финансы: Теория и Практика. − 2006. − №3. − URL: https://cyberleninka.ru/article/n/o-sisteme-obucheniya-studentov-osnovam-informatsionnoy-bezopasnosti (дата обращения: 02.12.2023).

41. Программа развития ГБПОУ «Южно-Уральский государственный технический колледж» на 2019-2023 гг. от 26.02.2019 г. № 03/668.

42. Разработка нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности [Электронный ресурс]: [методический документ ФСБ России: от 31.05.2015 г. № 149/7/2/6-432]. − Режим доступа: https://docs.cntd.ru (дата обращения: 20.10.2023).

43. Рапацевич Е.С. Педагогика. Большая современная энциклопедия / Е. С. Рапацевич. − Москва: Современное слово, 2010.

44. Салихов А.Т. Проектирование и разработка электронного практикума / А.Т. Салихов. − URL: http://fcoit.ru/internet_conference/the_development_of_electronic_teaching_materials_in_the_learning_process/proektirovanie_i_razrabotka_elektronnogo_praktikuma.php (дата обращения: 18.11.2023).

45. Технологии обеспечения информационной безопасности в образовательном учреждении (организации): метод. рекомендации для руководителей и педагогов образовательных учреждений (организаций) / авт.-сост. Н.Ю. Сероштанова, Е.В. Тюгаева, Н.В. Шпарута: Государственное автономное образовательное учреждение дополнительного профессионального образования Свердловской области «Институт развития образования». - Екатеринбург: ГАОУ ДПО СО «ИРО», 2014. -44 с.

46. Шумекеева Г. Б. Защита персональных данных как одна из проблем современного мира / Г. Б. Шумекеева // Право: современные тенденции: материалы VI Междунар. науч. конф. (г. Краснодар, октябрь 2018 г.). - Краснодар: Новация, 2018. - С. 47-49.